目　录

第一章　有限域

§1.1　来自初等数论的例子

我们在引言中说过，利用初等数论，对每个素数 p，可以构作出一个 p 元域 F_p. 在这节中我们利用初等数论更详细地讲述这些 p 元域和它们的性质，为今后讲述更一般的有限域增加些感性知识. 让我们先从初等数论的一些基本事实讲起.

初等数论的基本研究对象是自然数集合

$$N = \{0,1,2,3,\cdots\}$$

和整数集合

$$Z = \{0, \pm 1, \pm 2, \pm 3,\cdots\}.$$

整数集合 Z 中可以作加减乘三种运算，其中加法和乘法均有结合律和交换律，加法与乘法之间还有分配律. 但是 Z 中作除法并不总是可行的. 换句话说，设 a 和 b 为两个整数，其中 $b\neq 0$. 则 $\frac{a}{b}$ 不一定是整数. 如果 $\frac{a}{b}$ 是整数，我们称 b 整除 a，表示成 $b|a$.

否则，即若$\frac{a}{b}$不是整数，便称 b 不能整除 a，表示成 $b\nmid a$. 例如 $(-2)\mid 6$，$2\nmid 3$，而 ± 1 可以整除任何整数，每个非零整数均可以整除 0，等等.

如果 $a,b\in \mathbf{Z}$，$b\neq 0$，$b\mid a$，我们称 b 是 a 的一个**因子**，a 叫作 b 的一个**倍数**. 每个非零整数 n 都有因子 ± 1 和 $\pm n$. 设 p 是一个大于 1 的正整数. 如果 p 的正因子只有 1 和 p，换句话说，p 不能写成两个正整数之积，而这两个正整数因子均小于 p，便称 p 为**素数**.

每一门学问都有几个最基本的结果作为这门学科的基石. 初等数论的基石是下面的算术基本定理，我们假定大家熟悉它，证明从略.

1.1.1 算术基本定理 每个大于 1 的正整数 n 均可写成有限个素数的乘积：

$$n = p_1p_2\cdots p_s.$$

并且若不计素因子 $p_1,\cdots,p_s$ 的次序，这个分解式是唯一的.

如果我们把相同的素因子收集在一起，则上式可以写成

$$n = p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r},$$

其中 $p_1,\cdots,p_r$ 是彼此不同的素数，而 $a_i\geqslant 1(1\leqslant i\leqslant r)$. 这叫作正整数 n 的**标准分解式**.

初等数论的另一块基石，便是(欧几里德)除法算式.

1.1.2 除法算式 设 $a,b\in \mathbf{Z}$，$b>0$，则存在唯一的整数 q 和 r，使得 $a=qb+r$，并且 $0\leqslant r<b$.

我们也假定读者熟悉这个除法算式而不加证明(虽然证明是很容易的). 只想再指出，如果 a 也是正整数，那么除法算式中

的 q 就是用 b 除 a 得到的商，而 r 是余数.

设 $a_1, a_2, \cdots, a_n$ 是不全为零的 n 个整数. 由于每个非零整数只有有限多个因子，所以当 $a_1, \cdots, a_n$ 不全为零时，它们也只有有限多个公因子. 我们用 $(a_1, \cdots, a_n)$ 表示 $a_1, \cdots, a_n$ 的最大公因子. 如果 $(a_1, \cdots, a_n) = 1$，便称这 n 个整数 $a_1, \cdots, a_n$ 是**互素**的. 下面几条关于最大公因子的性质可由定义直接推出（设 a、b、c 均为非零整数）：

(1) $(a,b) = (b,a)$；

(2) $(a,b,c) = ((a,b),c)$；

(3) $b|a \Longleftrightarrow (a,b) = b$（这里 $A \Longleftrightarrow B$ 表示命题 A 和命题 B 彼此等价）；

(4) $(a,b) = (a,b+ac)$.

但是，下一个结果是不平凡的：

1.1.3 定理 设 a 和 b 是不全为零的整数，则对每个整数 n，不定方程

$$ax + by = n \qquad (*)$$

有整数解 (x,y) 的充要条件是 $(a,b)|n$，特别地，方程 $ax + by = 1$ 有整数解的充要条件是 $(a,b) = 1$.

证明 我们用 S 表示所有形如 $am + bs$ 的整数所成的集合，其中 $m, s \in \mathbf{Z}$. 即

$$S = \{am + bs | m, s \in \mathbf{Z}\},$$

于是：方程 $(*)$ 有整数解 $\Longleftrightarrow n \in S$. 集合 S 有如下一些特性：

(1) 若 $n, n' \in S$，则 $n \pm n' \in S$.

这是因为存在整数 m, m', s, s'，使得 $n = am + bs$，$n' = am' + bs'$. 于是 $n \pm n' = a(m \pm m') + b(s \pm s') \in S$.

(2) 若 $n \in S$，则对每个整数 c，$cn \in S$.

这是因为存在整数 m 和 s，使得 $n = am + bs$. 于是

$$cn = a(cm) + b(cs) \in S.$$

(3)设 d 为集合 S 中的最小正整数，则 S 恰好是 d 的所有倍数所成的集合.

由于 a 和 b 不全为零，并且 $a = a \cdot 1 + b \cdot 0 \in S, b = a \cdot 0 + b \cdot 1 \in S$. 由(2) 知 $\pm a$, $\pm b \in S$. 因此 S 中必包含正整数. 我们以 d 表示 S 中最小的正整数. 由(2) 知 d 的每个倍数均属于 S. 反之，对于 S 中每个数 n，利用除法算式知 $n = qd + r$，其中 $q, r \in \mathbf{Z}$，并且 $0 \leqslant r \leqslant d-1$. 由于 $d \in S$，由(2)知 $qd \in S$. 又因为 $n \in S$，再由(1)知 $r = n - qd \in S$. 但是 $0 \leqslant r \leqslant d-1$，而 d 是 S 中最小的正整数，所以必然 $r = 0$，即 $n = qd$，因此 n 为 d 的倍数. 这就证明了 S 恰好是 d 的全体倍数构成的集合.

(4) $d = (a, b)$.

记 $D = (a, b)$. 由于 $d \in S$，从而有整数 m, s，使得 $d = am + bs$. 因为 $D \mid a, D \mid b$，从而 $D \mid am + bs = d$. 特别地，$D \leqslant d$. 另一方面，由于 $a, b \in S$（见(3)的证明），根据(3)可知 $d \mid a, d \mid b$. 于是 d 为 a 和 b 的公因子，它当然不超过 a 和 b 的最大公因子 D. 于是 $d \leqslant D$. 因此 $d = D = (a, b)$.

性质(3)和(4)表明，集合 S 恰好是由 (a, b) 的所有倍数构成的集合. 于是：不定方程 $ax + by = n$ 有整数解 $\Longleftrightarrow n \in S \Longleftrightarrow (a, b) \mid n$. 这就证明了定理 1.1.3.

由定理 1.1.3 可以推出最大公因子的一系列性质.

1.1.4 定理 设 a 和 b 是不全为零的整数.

(1) 若 m 为正整数，则 $(ma, mb) = m(a, b)$.

(2) 若 $(a, b) = d$，则 a/d 和 b/d 是互素的整数.

(3) a 和 b 的每个公因子都是其最大公因子 (a, b) 的因子.

(4) 若$(a,m)=1$，$(b,m)=1$，则$(ab,m)=1$.

(5) 若$c|ab$，$(c,b)=1$，则$c|a$. 特别地，若p为素数，$p|ab$，$p\nmid b$，则$p|a$.

证明 (1)根据定理 1.1.3 可知

(ma,mb)=形如$max+mby$的最小正整数

$=m\cdot$(形如$ax+by$的最小正整数)

$=m(a,b)$.

(2)显然$\frac{a}{d},\frac{b}{d}\in\mathbf{Z}$，并且由(1)知

$$d=(a,b)=\left(d\cdot\frac{a}{d},d\cdot\frac{b}{d}\right)=d\left(\frac{a}{d},\frac{b}{d}\right).\text{于是}\left(\frac{a}{d},\frac{b}{d}\right)=1.$$

(3)若m为a和b的公因子，则$a=ma'$，$b=mb'$，其中a'，$b'\in\mathbf{Z}$. 于是$(a,b)=(ma',mb')=m(a',b')$. 即m为(a,b)的因子.

(4) 由$(a,m)=(b,m)=1$可知存在$x,y,x',y'\in\mathbf{Z}$，使得$ax+my=1$，$bx'+my'=1$(定理 1.1.3). 于是

$$ab(xx')+m(axy'+bx'y+myy')$$
$$=(ax+my)(bx'+my')=1.$$

再由定理 1.1.3 即知$(ab,m)=1$.

(5)如果$c|ab$，又显然有$c|ac$. 由(4)可知$c|(ab,ac)=a(b,c)=a$，即$c|a$. 特别若p为素数，$p|ab$. 如果$p\nmid b$，则$(p,b)=1$. 因此$p|a$.

现在讲整数的同余性质. 设m是正整数，a和b是任意整数. 如果$m|(a-b)$，我们便说a和b模m**同余**，并且表示成$a\equiv b\pmod m$. 这时，用除法算式将m去除a和b时有同样的余数r. 如果$m\nmid(a-b)$，称a和b模m不同余，表示成$a\not\equiv b\pmod m$. 例如$5\equiv-1\pmod 3$，$-1\not\equiv 6\pmod 8$. 显然$a\equiv 0\pmod m\Longleftrightarrow$

$m\mid a$.

下面是同余式的一些简单性质.

1.1.5 引理 (1) $a\equiv a \pmod m$;

(2) 若 $a\equiv b \pmod m$,则 $b\equiv a \pmod m$;

(3) 若 $a\equiv b \pmod m$, $b\equiv c \pmod m$,则 $a\equiv c \pmod m$;

(4) 若 $ac\equiv bc \pmod m$,则 $a\equiv b\left(\bmod \dfrac{m}{(c,m)}\right)$. 特别当 $(c,m)=1$ 时,由 $ac\equiv bc \pmod m$ 得到 $a\equiv b \pmod m$;

(5) 若 p 为素数, $ac\equiv bc \pmod p$,并且 $p\nmid c$,则 $a\equiv b \pmod p$.

证明 前三条很容易验证,现在证(4):由 $ac\equiv bc \pmod m$ 可知 $m\mid ac-bc=(a-b)c$. 记 $d=(c,m)$,则 $\frac{m}{d},\frac{c}{d}\in\mathbf{Z}$,并且 $\frac{m}{d}\mid(a-b)\cdot\frac{c}{d}$. 但是 $\left(\frac{m}{d},\frac{c}{d}\right)=1$(定理 1.1.4 的(2)),从而 $\frac{m}{d}\mid(a-b)$(定理 1.1.4 的(5)). 于是 $a\equiv b\left(\bmod \frac{m}{d}\right)$. 这就证明了(4). 而(5)可由(4)直接推出.

现在我们固定一个正整数 $m\geqslant 2$. 对每个整数 a,用 $[a]$ 表示模 m 与 a 同余的所有整数构成的集合,叫作模 m 的一个**同余类**. 即

$$\begin{aligned}[a]&=\{c\in\mathbf{Z}\mid c\equiv a \pmod m\}\\&=\{c,c\pm m,c\pm 2m,c\pm 3m,\cdots\}.\end{aligned}$$

不难看出, $[a]=[b]\Longleftrightarrow a\equiv b \pmod m$. 由于每个整数模 m 均同余于 $0,1,\cdots,m-1$ 当中的一个数(除法算式!). 从而一共有 m 个同余类 $[0]$、$[1]$,$\cdots$,$[m-1]$. 我们可以自然地在这些同余类上作加减乘法运算,即定义

$[a]+[b]=[a+b]$, $[a]-[b]=[a-b]$, $[a]\cdot[b]=[a\cdot b]$. 则[0]起着通常数 0 的作用,即

$$[0]+[a]=[a], \quad [0]\cdot[a]=[0].$$

而减法是加法的逆运算. 即

若$[a]+[b]=[c]$,则$[c]-[a]=[b]$.

并且加法和乘法均满足交换律和结合律,也有分配律:

$[a]([b]+[c])=[a][b]+[a][c]$(均等于$[ab+ac]$).

而[1]在乘法中起着数 1 的作用,即

$$[1]\cdot[a]=[a].$$

我们现在考查一下在模 m 的同余类中间是否有乘法的逆运算——除法. 首先看看每个同余类$[a]$($\neq[0]$)是否可以去除[1],即是否存在同余类$[b]$,使得$[a]\cdot[b]=[1]$.

1.1.6 引理 设 $m\geqslant 2$,$[a]$为模 m 的同余类,则存在同余类$[b]$使得$[a]\cdot[b]=[1]$的充要条件是$(a,m)=1$. 并且当$(a,m)=1$时,只有一个同余类$[b]$使得$[a]\cdot[b]=[1]$.

证明 若$[a]\cdot[b]=[1]$,则$[ab]=[1]$,从而 $ab\equiv 1 \pmod m$. 于是有 $n\in\mathbf{Z}$,使得 $ab-1=mn$. 设 $d=(a,m)$,则 $d\mid ab-mn=1$,因此 $d=1$,即$(a,m)=1$. 反之,若$(a,m)=1$. 则有 $b,y\in\mathbf{Z}$,使得 $ab+my=1$(定理 1.1.3). 于是 $1=ab+my\equiv ab \pmod m$,即$[a]\cdot[b]=[ab]=[1]$. 最后我们证明$[b]$的唯一性:若$[a]\cdot[b]=1$,$[a]\cdot[b']=1$,则 $ab\equiv 1\equiv ab' \pmod m$,由于$(a,m)=1$,从而 $b\equiv b' \pmod m$(引理 1.1.5 的(4)). 于是$[b]=[b']$. 这就证明了引理 1.1.6.

如果 m 不是素数,则 m 有正因子 d,使得 $1<d<m$. 于是$[d]\neq[0]$,并且由于$(m,d)=d>1$,根据引理 1.1.6 可知不存在

$[b]$，使得$[d]\cdot[b]=[1]$. 换句话说，在模 m 的同余类集合中不能用$[d]$($\neq[0]$)去除$[1]$，所以除法不总是可行的. 但是当 m 为素数 p 时，如果$[a]\neq[0]$，即 $a\not\equiv 0(\bmod p)$，则$(p,a)=1$. 从而存在唯一的模 p 同余类$[b]$，使得$[a]\cdot[b]=[1]$.（引理 1.1.6）. 我们称$[b]$为$[a]$的**逆**，并且表示成$[a]^{-1}$，于是当$[a]\neq[0]$时，

$$[a]\cdot[a]^{-1}=[a]^{-1}\cdot[a]=[1].\left(\text{即}[a]^{-1}=\frac{[1]}{[a]}\right)$$

这时对任意模 p 同余类$[c]$，均可用$[a]$去除$[c]$，即存在唯一的同余类$[x]$，使得$[a]\cdot[x]=[c]$. 事实上，$[x]=[a]^{-1}\cdot[c]$. 这就表明，如果以 F_p 表示模 p 的 p 个同余类$[0],\cdots,[p-1]$所构成的集合，则 F_p 上有四则运算，并且这些运算满足通常的运算法则. 换句话说，F_p 是一个域，这是由 p 个元素组成的有限域，其中 p 为任意素数.

我们举 F_7 为例. 加法减法和乘法是很容易作的，例如$[2]+[6]=[8]=[1]$，$[2]-[6]=[2-6]=[-4]=[3]$，$[2]\cdot[6]=[12]=[5]$，等等. 我们有如下的乘法表：

	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[2]	[0]	[2]	[4]	[6]	[1]	[3]	[5]
[3]	[0]	[3]	[6]	[2]	[5]	[1]	[4]
[4]	[0]	[4]	[1]	[5]	[2]	[6]	[3]
[5]	[0]	[5]	[3]	[1]	[6]	[4]	[2]
[6]	[0]	[6]	[5]	[4]	[3]	[2]	[1]

除法运算则不简单（特别当 p 是大素数的时候），因为求$[x]=\frac{[a]}{[b]}$($[b]\neq[0]$)相当于解同余方程 $bx\equiv a(\bmod\ p)$. 例如为求

$\frac{[2]}{[5]}$，我们可藉助于乘法表，在最左边一列中找到[5]，将这个[5]所在那一行的栏内找到[2]，则位于[2]的最上方是[6]，于是 $[5]\cdot[6]=[2]$，即 $\frac{[2]}{[5]}=[6]$. 我们也可以解同余方程 $5x\equiv 2 \pmod 7$. 它等价于 $5x\equiv 2+4\cdot 7=30 \pmod 7$，由于 $(5,7)=1$，从而 $x\equiv\frac{30}{5}\equiv 6 \pmod 7$. 即 $\frac{[2]}{[5]}=[6]$. 这也可以写成

$$\frac{[2]}{[5]}=\frac{[2+28]}{[5]}=\frac{[30]}{[5]}=\left[\frac{30}{5}\right]=[6].$$

现在我们谈谈 p 元有限域 F_p 一些有趣的性质. 为了符号简单，对于固定的素数 p，今后我们把模 p 同余类 $[a]$ 简写作 a. 于是，作为 F_p 中的元素 a 和 b，$a=b$ 是指 $a\equiv b \pmod p$. 于是在 F_p 中便得到第一个有趣的等式：$p=0$. 由此又得出下面有趣结果：

1.1.7 定理 设 $a,b\in \boldsymbol{Z}$，则在 p 元域 F_p 中，

$$(a+b)^p=a^p+b^p.$$

证明 我们应当有二项式展开

$$(a+b)^p=a^p+C_p^1a^{p-1}b+\cdots+C_p^{p-1}ab^{p-1}+b^p.$$

其中 $C_p^i=\frac{p!}{i!\,(p-i)!}$ 是整数. 但是当 $1\leqslant i\leqslant p-1$ 时，$1\leqslant p-i\leqslant p-1$. 因此 p 除不尽 C_p^i 的分母 $i!\,(p-i)!$，可是分子 $p!$ 有因子 p，于是 $p\mid C_p^i$（对于 $1\leqslant i\leqslant p-1$）. 于是在 F_p 中 $C_p^i=0$（$1\leqslant i\leqslant p-1$）. 所以若将二项式展开式看成 F_p 中的等式，右边只剩下前后两项，即 $(a+b)^p=a^p+b^p$.

1.1.8 定理 对于 F_p 中每个元素 a，均有等式 $a^p=a$. 如果 $a\neq 0$（在 F_p 中），则 $a^{p-1}=1$.

证明 首先指出，在域 F_p 中也有下面的消去律：若 $a,b,c\in$

$F_p, a\neq 0$,则由 $ab=ac$ 可推出 $b=c$. 这是由于 $a\neq 0$,从而存在逆元素 a^{-1}. 于是

$$b=1\cdot b=(a^{-1}\cdot a)\cdot b=a^{-1}\cdot(a\cdot b)\quad(\text{结合律})$$
$$=a^{-1}\cdot(ac)=(a^{-1}a)c=1\cdot c=c.$$

仍设 $a\neq 0$. 则 $1,2,\cdots,p-1$ 是 F_p 中全部非零元素,易知 a, $2a,3a,\cdots,(p-1)a$ 是 F_p 中不同的元素(利用上面的消去律),并且均不为 0(仍用消去律:若 $ia=0=i\cdot 0, 1\leqslant i\leqslant p-1$. 由于 $i\neq 0$,从而 $a=0$,这与假设 $a\neq 0$ 相矛盾). 于是 $a,2a,\cdots,(p-1)a$ 也是 F_p 中全部非零元素,所以在 F_p 中便有等式

$$1\cdot 2\cdot\cdots\cdot(p-1)=a\cdot(2a)\cdot\cdots\cdot(p-1)a.$$

即 $1\cdot 2\cdot\cdots\cdot(p-1)=1\cdot 2\cdot\cdots\cdot(p-1)\cdot a^{p-1}$. 由于 $1\cdot 2\cdot\cdots\cdot(p-1)\neq 0$,因此用消去律即知 $a^{p-1}=1$(当 $a\neq 0$ 时),从而 $a^p=a$. 而后一等式显然对 $a=0$ 也成立. 这就证明了定理 1.1.8.

注记 将定理 1.1.8 叙述成同余式的语言,则是:设 p 为素数,$a\in \mathbf{Z}, p\nmid a$,则 $a^{p-1}\equiv 1 \pmod p$. 这正是初等数论中的费尔马小定理.

1.1.9 定义 设 a 是 F_p 中非零元素. 则使等式 $a^n=1$ 成立的最小正整数 n 叫作元素 a 的阶,而 a 叫作 F_p 中的 n 阶元素. (由于 $a^{p-1}=1$,从而必存在最小正整数 n 使得 $a^n=1$.)

例如在 F_7 中,1 是 1 阶元素,6(=-1)是 2 阶元素,2 和 4 是 3 阶元素,3 和 5 是 6 阶元素.

1.1.10 定理 设 a 是 F_p 中 n 阶(非零)元素. 则

(1) 对每个整数 N, $a^N=1\Longleftrightarrow n\mid N$. 特别地,$F_p$ 中非零元素 a 的阶均是 $p-1$ 的因子.

(2) 对每个整数 m，元素 a^m 的阶是$\frac{n}{(n,m)}$. 特别地，a^m 为 n 阶元素的充要条件是$(n,m)=1$.

证明 (1)若 $n|N$，则有 $k\in\mathbf{Z}$，使得 $N=kn$. 于是 $a^N=a^{nk}=(a^n)^k=1^k=1$. 反之，若 $a^N=1$. 由除法算式可知 $N=qn+r$，其中 $q,r\in\mathbf{Z}$，$0\leqslant r\leqslant n-1$. 于是

$$a^r=a^{N-qn}=a^N\cdot(a^n)^{-q}=1\cdot(1)^{-q}=1.$$

由于 n 是满足 $a^n=1$ 的最小正整数，而 $0\leqslant r\leqslant n-1$. 所以必然 $r=0$，即 $N=qn$. 于是 $n|N$. 最后，由于 $a^{p-1}=1$(定理 1.1.8)，因此 $n|(p-1)$.

(2)对于每个正整数 l，

$$\begin{aligned}(a^m)^l=1\Longleftrightarrow a^{ml}=1\Longleftrightarrow n|ml \quad &(\text{由本定理的}(1))\\ \Longleftrightarrow \frac{n}{(n,m)}\left|\frac{m}{(n,m)}\cdot l\right.&\\ \Longleftrightarrow \frac{n}{(n,m)}\Big|l \quad &\left(\text{由于}\frac{n}{(n,m)}\text{和}\frac{m}{(n,m)}\text{互素}\right).\end{aligned}$$

而元素 a^m 的阶是满足$(a^m)^l=1$ 的最小正整数 l. 于是它也是满足$\frac{n}{(n,m)}\Big|l$ 的最小正整数 l，这显然为$\frac{n}{(n,m)}$. 最后，

$$a^m\text{ 的阶为}n\Longleftrightarrow\frac{n}{(n,m)}=n\Longleftrightarrow(n,m)=1.$$

注记 根据定理 1.1.10，有限域 F_p 中每个非零元素的阶都是 $p-1$ 的因子. 例如在 F_7 中，非零元素的阶只能是 6 的因子，即 F_7 中只能有 6 阶，3 阶，2 阶和 1 阶元素(见前面的例子).

假如 F_p 中存在 $p-1$ 阶元素 g，那么 $1=g^0,g^1,g^2,\cdots,g^{p-2}$ 便是 F_p 中 $p-1$ 个彼此不同的非零元素(因为若 $g^i=g^j$，$0\leqslant i\leqslant j\leqslant p-2$，则 $j-i\geqslant 0$ 并且 $j-i\leqslant p-2$. 而 $g^{j-i}=g^j\cdot(g^i)^{-1}=g^i(g^i)^{-1}=1$. 由于 g 的阶为 $p-1$ 而 $0\leqslant j-i\leqslant p-2$，从而必然 $j-i=0$，即 $j=i$). 所以 F_p 中每个非零元素均是 g 的方幂. 从而

F_p 有非常简单的乘法结构，F_p 中的 $p-1$ 阶元素 g 在初等数论中叫作模 p 的**原根**. 并且在初等数论中证明了：对每个素数 p，必存在模 p 的原根，换句话说，有限域 F_p 中一定有 $p-1$ 阶元素. 这样的元素叫作 F_p 中的**本原元素**. 我们在第 1.4 节中将要对任意有限域证明类似的结论.

现在我们暂且假定 F_p 中存在本原元素 g. 于是 F_p 中 $p-1$ 个非零元素为$g^1,g^2,\cdots,g^{p-1},g^{p-1}=g^0=1$. F_p 中可能有许多个本原元素. 事实上，根据定理 1.1.10，非零元素 $g^i(1\leqslant i\leqslant p-1)$的阶为$\frac{p-1}{(p-1,i)}$. 从而 g^i 是本原元素的充要条件为$(p-1,i)=1$. 即 F_p 中本原元素的个数恰好是 $1,2,3,\cdots,p-1$ 当中与 $p-1$ 互素的数的个数. 在初等数论中，对每个正整数 n，我们用 $\varphi(n)$表示 $1,2,\cdots,n$ 当中与 n 互素的数的个数. 这叫作**欧拉函数**. 例如 $\varphi(1)=1,\varphi(2)=1,\varphi(3)=2,\varphi(4)=2,\varphi(5)=4,\varphi(6)=2,\varphi(7)=6$ 等等. 于是，F_p 中共有 $\varphi(p-1)$个本原元素. 例如在 F_7 中共有 $\varphi(7-1)=\varphi(6)=2$ 个本原元素，它们是 3 和 5.

给了一个大素数 p，如何快速地求出 F_p 中的一个本原元素 g? 进而，如果知道了 F_p 中一个本原元素 g，那末对 F_p 中每个非零元素 a，如何快速地求出使 $a=g^i$ 成立的指数 i? 这些都是工程技术上非常感兴趣的算法问题. 数论学家阿廷(E. Artin)曾经提出一个猜想：对每个大于 1 的非平方整数 a，均存在无限多个素数 p，使得 a 是有限域 F_p 中的本原元素. 这个猜想至今未能解决. 此外，估计模 p 最小原根 g 的上界(或者$|g|$的上界)也是一个很难的理论问题. 我国数论学家王元等人在这方面曾作过好的结果，但是离猜想的上界还有很大距离. 有兴趣的读者请看华罗庚:《数论导引》一书.

关于 p 元有限域暂且讲到这里.

1.1.11 习　题

1. 设 a 和 b 均是非零整数，以 $[a,b]$ 表示 a 和 b 的最小(正)公倍数. 求证

   (Ⅰ) a 和 b 的每个公倍数都是 $[a,b]$ 的倍数.

   (Ⅱ) 若 m 为正整数，则 $[ma,mb]=m[a,b]$.

   (Ⅲ) $(a,b)[a,b]=ab$. 特别地，a 和 b 互素的充要条件是 $[a,b]=ab$.

2. 设 a 和 b 是互素的整数. 令 (x_0,y_0) 为不定方程 $ax+by=1$ 的一组整数解(整数解的存在性由定理 1.1.3 所保证)，则该方程的全部整数解可以表示成 $x=x_0+bt, y=y_0-at$，其中 t 为任意整数.

3. 求下列方程全部整数解：

   (Ⅰ) $243x+198y=909$;　　(Ⅱ) $41x-114y=5$.

4. 证明素数有无限多个。

5. 在 F_{37} 中作除法 $\frac{[7]}{[60]}=?$

6. 设 p 为素数，k 和 l 为正整数，求证 $(p^k-1,p^l-1)=p^{(k,l)}-1$.

7. 求有限域 F_{13} 中的所有本原元素，3 阶元素和 4 阶元素.

8. 设 a 和 b 为有限域 F_p 中的非零元素. 求证

   (Ⅰ) a 和 a^{-1} 有相同的阶.

   (Ⅱ) 若 a 和 b 的阶分别为 s 和 t，并且 $(s,t)=1$，则 ab 的阶为 st.

   (Ⅲ) 若 a 为 3 阶元素，则 $a^2+a+1=0$，并且 $1+a$ 为 6 阶元素.

   (Ⅳ) a 的阶数为 n 的充要条件是：$a^n=1$，并且对 n 的每个素因子 p，$a^{\frac{n}{p}}\neq 1$.

9. 验证 257 是素数，并且 10 是域 F_{257} 中的本原元素.

10. 设 p 为素数，并且 $p\equiv 1 \pmod 4$. 求证：若 g 是 F_p 中本原元素，则 $-g$ 也是 F_p 中本原元素.

11. 设 m 为任意正整数，以 $[a]$ 表示整数 a 的模 m 同余类. 求证

    (Ⅰ) 共有 $\varphi(m)$ 个乘法可逆的模 m 同余类 $[a]$，其中 $\varphi(m)$ 是欧拉函数.（$[a]$ 叫乘法可逆的，是指存在 $b\in \mathbf{Z}$，使得 $[a][b]=[1]$）.

    (Ⅱ) 若 $[a_1],[a_2],\cdots,[a_{\varphi(m)}]$ 是所有乘法可逆的模 m 同余类，则对每个与 m 互素的整数 a，$[aa_1],[aa_2],\cdots,[aa_{\varphi(m)}]$ 也是所有乘法可逆的模

m 同余类.

(Ⅱ)(小费尔马定理)设 a 为整数,$(a,m)=1$. 求证 $a^{\varphi(m)}\equiv 1 \pmod{m}$.

12. 求证:(Ⅰ)对每个大于 3 的正整数 m,$\varphi(m)$均是偶数.(Ⅱ)若 p 为素数,$n\geqslant 1$. 则 $\varphi(p^n)=p^{n-1}(p-1)$.

§1.2　什么是域?

我们曾说,域是具有四则运算的集合,并且这些运算满足通常一些运算法则. 但是这个说法是非常不准确的. 这一节我们首先给出域的确切定义. 有了有理数域、实数域、复数域和有限域 $\boldsymbol{F}_p$ 这样一些实际例子,下面对域作公理化的定义时就不会感到抽象和空泛.

1.2.1　定义　设 F 是一个集合,并且在集合 F 上规定了两种运算,叫作加法和乘法. 即对于 F 中任意两个元素 a 和 b,作加法运算得到 F 中唯一元素 $a+b$,作乘法运算得到 F 中唯一元素 $a\cdot b$(或简写作 ab). 我们说集合 F 对于所规定的加法和乘法运算是一个域,是指以下运算规则都成立:

(Ⅰ)关于加法:

(Ⅰ.1)(结合律)$(a+b)+c=a+(b+c)$

(对任意 $a,b,c\in F$).

(Ⅰ.2)(交换律)$a+b=b+a$　(对任意 $a,b\in F$).

(Ⅰ.3)(零元素)在 F 中存在元素,记成 0,使得

$a+0=a$　(对每个 $a\in F$).

(注意:满足这性质的 0 至多只有一个,因为若 F 中元素 $0'$ 也有此性质,即 $a+0'=a$(对每个 $a\in F$),那末 $0+0'$ 既等于 0,

又应当等于 $0'$，从而 $0=0'$）.

（Ⅰ.4）（负元素）对每个元素 $a\in F$，均有 $b\in F$，使得

$$a+b=0.$$

（注意：满足此性质的 b 也是唯一的，因若 $a+b'=0$，则 $b'=b'+0=b'+(a+b)=(b'+a)+b=0+b=b$）.

我们把满足 $a+b=0$ 的唯一元素 b 记成 $(-a)$，叫作 a 的负元素. 于是 $b+(-b)=0$.（若把 a 与 $(-b)$ 之和表成 $a-b$，即 $a+(-b)=a-b$. 从而 F 中有减法运算.）

（Ⅱ）关于乘法：

（Ⅱ.1）（结合律）$(ab)c=a(bc)$（对任意 $a,b,c\in F$）.

（Ⅱ.2）（交换律）$ab=ba$（对任意 $a,b\in F$）.

（Ⅱ.3）（幺元素）在 F 中存在元素（记作）1，$1\neq 0$，使得 $a\cdot 1=a$（对每个 $a\in F$）.

（满足上述性质的幺元素也至多只有 1 个，因若 $a\cdot 1'=a$（对每个 $a\in F$），则 $1\cdot 1'$ 既等于 1，又等于 $1'$，从而 $1=1'$）.

（Ⅱ.4）（逆元素）对于 F 中每个元素 $a\neq 0$，均有 $b\in F$，使得 $ab=1$.

（满足上述性质的 b 是唯一的，因若 $ab'=1$，则 $b=b\cdot 1=b(ab')=(ba)b'=(ab)b'=1\cdot b'=b'$.）满足 $ab=1$ 的唯一元素 b 表示成 a^{-1}，叫作 a 的逆元素.（于是当 $a,b\in F$，$a\neq 0$ 时，我们又有除法 $\frac{b}{a}=b\cdot a^{-1}$.）

（Ⅲ）（分配律）$a(b+c)=ab+ac$（对任意 $a,b,c\in F$）.

有理数集合、实数集合与复数集合对于通常数的加法和乘法运算满足上述全部法则，所以它们都是域. 其中零元素和幺元素分别是数 0 和 1. 对每个素数 p，我们在前节表明集合 F_p 对于

同余类的加法和乘法运算也满足上述全部法则，所以也是域．而零元素和幺元素分别是同余类[0]和[1]．为了扩大眼界，我们再举一些域的例子．

例 1 我们以 $\boldsymbol{R}$ 表示实数域．考虑集合

$$\boldsymbol{R}[\sqrt{-2}]=\{a+b\sqrt{-2}\mid a,b\in\boldsymbol{R}\}.$$

这是复数域的一个子集，这个集合里可以定义通常复数的加法和乘法运算．这需要验证：$\boldsymbol{R}[\sqrt{-2}]$中任意两个数的和与积仍旧属于 $\boldsymbol{R}[\sqrt{-2}]$．事实上，若 $\alpha=a+b\sqrt{-2}$，$\beta=c+d\sqrt{-2}$ 为 $\boldsymbol{R}[\sqrt{-2}]$中的数，其中 $a,b,c,d\in\boldsymbol{R}$．则

$$\alpha+\beta=(a+c)+(b+d)\sqrt{-2},$$

$$\alpha\beta=(ac-2bd)+(ad+bc)\sqrt{-2}.$$

可知 $\alpha+\beta,\alpha\beta\in\boldsymbol{R}[\sqrt{-2}]$．于是通常数的加法和乘法确实是集合 $\boldsymbol{R}[\sqrt{-2}]$中的运算．现在我们验证域的定义中的那些公理．多数公理是容易验证的，$\boldsymbol{R}[\sqrt{-2}]$中的零元素和幺元素仍是数 0 和 1．$a+b\sqrt{-2}$的负元素为$-a-b\sqrt{-2}$．关键是验证公理(Ⅰ.4)，即对 $\boldsymbol{R}[\sqrt{-2}]$中每个非零元素 $\alpha=a+b\sqrt{-2}$(从而 a 和 b 是不全为零的实数)，我们要证存在 $\beta\in\boldsymbol{R}[\sqrt{-2}]$，使得 $\alpha\beta=1$．首先因为 $\alpha\neq0$，从而必有复数 β，使得 $\alpha\beta=1$(因为复数全体是域!)，由于

$$\beta=\alpha^{-1}=\frac{1}{a+b\sqrt{-2}}=\frac{a-b\sqrt{-2}}{a^2+2b^2}$$

$$=\left(\frac{a}{a^2+2b^2}\right)+\left(\frac{-b}{a^2+2b^2}\right)\sqrt{-2}.$$

并且 $a^2+2b^2\neq0$(因为 a 和 b 是不全为零的实数)，从而$\frac{a}{a^2+2b^2}$，$\frac{-b}{a^2+2b^2}\in\boldsymbol{R}$．这就表明 $\beta\in\boldsymbol{R}[\sqrt{-2}]$．因此 α 在 $\boldsymbol{R}[\sqrt{-2}]$中有逆元素．于是 $\boldsymbol{R}[\sqrt{-2}]$是一个域．

例 2 设 F 是任意一个域. x 是一个文字(或叫未定元). 我们以 $F[x]$表示以 x 为未定元系数属于域 F 的所有多项式构成的集合. 即 $F[x]$中元素是多项式

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n.$$

其中 $a_i\in F(0\leqslant i\leqslant n)$. 如果 $a_0\neq 0$, 称 $f(x)$为 *n 次*多项式, a_0 叫 $f(x)$的*首项系数*. $F[x]$中两个多项式

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n,\quad g(x)=b_0x^n+b_1x^{n-1}+\cdots+b_n$$

相等, 是指对应系数均(在 F 中)相等, 即 $a_i=b_i$ $(0\leqslant i\leqslant n)$. 在多项式集合 $F[x]$中象通常那样定义加法和乘法, 即对 $F[x]$两个多项式

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n,\quad g(x)=b_0x^n+b_1x^{n-1}+\cdots+b_n,$$

其中 $a_i,b_j\in F$, 定义多项式加法为同次项系数相加:

$$f(x)+g(x)=(a_0+b_0)x^n+(a_1+b_1)x^{n-1}+\cdots+(a_n+b_n).$$

而多项式

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n,$$
$$g(x)=b_0x^m+b_1x^{m-1}+\cdots+b_m$$

相乘是用分配律之后再合并同类项:

$$f(x)g(x)=a_0b_0x^{n+m}+(a_0b_1+a_1b_0)x^{n+m-1}$$
$$+(a_0b_2+a_1b_1+a_2b_0)x^{n+m-2}+\cdots+a_nb_m.$$

易知这两个运算确实是 $F[x]$中的运算, 即若 $f(x),g(x)\in F[x]$, 则 $f(x)+g(x), f(x)g(x)\in F[x]$. 容易验证, 除了公理(Ⅱ.4)之外, $F[x]$对于上述运算满足所有其他公理. 这样的数学结构在数学上叫作是一个*环*(确切地说, 应叫作具有幺元素的交换环). 整数集合 **Z** 对于通常加法和乘法运算也是这样的环. 我们今后不准备多谈环的性质, 只是有时用一下*整数环* **Z** 或*多项式环* $F[x]$这样的名称.

正象引入有理分数可以将整数环 $\mathbf{Z}$ 扩大成有理数域一样，我们也可把多项式环用类似办法扩大成域. 设 $f(x)$ 和 $g(x)$ 是 $F[x]$ 中两个多项式，并且 $g(x)\neq 0$. 我们把 $\frac{f(x)}{g(x)}$ 叫作（系数属于 F 的）**有理函数**. 每个有理分数可以有许多种表示方法 $\left(\text{如}\frac{2}{3}=\frac{4}{6}=\frac{-6}{-9}\right)$，我们也需要把一些有理函数等同起来，即对于 $F[x]$ 中多项式 $f(x), g(x), f'(x), g'(x)$，其中 $g(x)\neq 0$, $g'(x)\neq 0$. 我们说有理函数 $\frac{f(x)}{g(x)}$ 和 $\frac{f'(x)}{g'(x)}$ **相等**，指的是 $f(x)g'(x)=f'(x)g(x)$. 以 $F(x)$ 表示系数属于域 F 的所有有理函数所成的集合，在 $F(x)$ 中如下定义加法和乘法（象分数一样）：

$$\frac{f(x)}{g(x)}+\frac{f'(x)}{g'(x)}=\frac{f(x)g'(x)}{g(x)g'(x)}+\frac{f'(x)g(x)}{g(x)g'(x)}$$
$$=\frac{f(x)g'(x)+f'(x)g(x)}{g(x)g'(x)},$$
$$\frac{f(x)}{g(x)}\cdot\frac{f'(x)}{g'(x)}=\frac{f(x)f'(x)}{g(x)g'(x)}.$$

当 $g(x)\neq 0, g'(x)\neq 0$ 时，易知 $g(x)g'(x)\neq 0$. 从而上述加法和乘法确实是 $F(x)$ 中的运算. 可以直接验证，$F(x)$ 对于这种加法和乘法运算满足域的所有公理（详细验证是不难但是相当烦琐，这里从略）. 比如说，对于有理函数 $\frac{f(x)}{g(x)}$，$g(x)\neq 0$. 如果 $\frac{f(x)}{g(x)}\neq 0$，则 $f(x)\neq 0$，而 $\frac{f(x)}{g(x)}$ 的逆元素就是 $\frac{g(x)}{f(x)}$. 从而公理（Ⅰ.4）满足. 于是 $F(x)$ 为域，叫作（以 F 为系数域的）**有理函数域**. 每个 F 中元素 a 可看成是 $F[x]$ 中的多项式，但是次数 ≥ 1 的多项式不属于 F. 因此多项式环 $F[x]$ 真包含域 F. 另一方面，每个多项式 $f(x)$ 可看成有理函数 $\frac{f(x)}{1}$，从而有理函数域 $F(x)$

又真包含 $F[x]$. 于是域 $F(x)$真包含域 F. 换句话说，对于每个域 F，我们都可作出一个比 F 更大的域 $F(x)$.

现在我们列出域的一些公共性质.

1.2.2 定理 设 F 是域，则

(1) (加法消去律)若 $a,b,c\in F$，$a+c=b+c$，则 $a=b$.

(2) (乘法消去律)若 $a,b,c\in F$，$c\neq o$，$ac=bc$，则 $a=b$.

(3) 对每个 $a\in F$，$a\cdot 0=0$.

(4) 设 $a,b\in F$，$ab=0$，则 $a=0$ 或者 $b=0$.

(5)对 $a,b\in F$，$-(-a)=a$，$-(a+b)=-a-b$，$a(-b)=(-a)b=-(ab)$，$(-a)(-b)=ab$.

(6)对于 F 中非零元素 a 和 b，

$$(a^{-1})^{-1}=a,\quad (ab)^{-1}=a^{-1}b^{-1},\quad (-a)^{-1}=-a^{-1}.$$

证明 我们只证明其中一部份作为例子，其余请读者自行补足.

(1) 若 $a+c=b+c$，则 $a+c+(-c)=b+c+(-c)$，但是 $c+(-c)=0$，从而 $a=b$. 类似可证乘法消去律(2).

(3) $a\cdot 0=a\cdot(0+0)=a\cdot 0+a\cdot 0$.

于是 $a\cdot 0=a\cdot 0-a\cdot 0=0$.

(4)设 $ab=0$，若 $a\neq 0$，则 $ab=a\cdot 0$，从而 $b=0$(由(2))，于是 a 和 b 至少有一个为零.

(6)由于 $ab(b^{-1}a^{-1})=a(bb^{-1})a^{-1}=a\cdot 1\cdot a^{-1}=a\cdot a^{-1}=1$，从而$(ab)^{-1}=b^{-1}a^{-1}=a^{-1}b^{-1}$. 由此推出

$(-a)^{-1}=((-1)a)^{-1}=(-1)^{-1}a^{-1}=-a^{-1}$.

注记 我们还可以推出下列一些法则：

(7) 对于 $a,b,c\in F$， $a-(b+c)=a-b-c$，

$a-(b-c)=a-b+c, \quad a(b-c)=ab-ac.$

(8) 设 $a\in F$，对于正整数 n，以 $n\cdot a$ 表示 n 个 a 相加，$0\cdot a=0$，$(-n)a=-(na)$. 则当 $n,m\in \mathbf{Z}$，$a,b\in F$ 时，$n(a+b)=na+nb$，$(m+n)a=ma+na$，$(mn)a=m(na)$，等等.

(9) 设 $a\in F$，n 为正整数，令 a^n 为 n 个 a 之积，$a^0=1$，$a^{-n}=(a^n)^{-1}$. 则对于 $a,b\in F$，$n,m\in \mathbf{Z}$，我们有 $a^{m+n}=a^m\cdot a^n$，$a^{mn}=(a^m)^n$， $(ab)^m=a^mb^m$， $(a+b)^n=\sum_{i=0}^{n}C_n^ia^ib^{n-i}$（其中 $n\geq 1$）.

这些运算法则都是大家所熟悉的，我们请读者自行证明. 现在我们再讲一些关于域的新性质.

1.2.3 定义 设 K 是域 F 的一个子集. 如果 K 对于 F 中规定的加法和乘法运算形成一个域，则 K 叫作 F 的子域，而 F 叫作 K 的扩域（或扩张）.

例如：有理数域是实数域的子域，而实数域又是复数域的子域. 对于每个域 F，有理函数域 $F(x)$ 是 F 的扩域. 记 $\mathbf{R}$ 为实数域，则 $\mathbf{R}[\sqrt{-2}]$ 是 $\mathbf{R}$ 的扩域.

注意子域 K 中的加法和乘法运算一定要和域 F 中的相同. 所以要验证域 F 的一个子集 K 是否为子域，首先要验证 K 中元素按 F 中运算作乘法和加法，所得的积与和是否仍属于 K. 若答案是肯定的，则 F 中的加法和乘法才可以看成是 K 中的运算. 其次要验证 K 对于加法和乘法运算是否满足域的诸条公理. 事实上，我们只需验证其中两条即可：若 $a\in K$，则 $-a$ 也属于 K；若 $a\in K$，$a\neq 0$，则（F 中元素）a^{-1} 也属于 K. 至于其他诸条公理，它们在 F 中成立，在 K 中也自然成立，所以是不用验证的.

1.2.4 定义 为了与数 1 相区别，我们暂时用 e 表示域 F 中的幺元素(于是对每个 $a\in F, ae=a$). 考查元素

$$e, 2e = e + e, 3e = e + e + e, \cdots.$$

如果存在正整数 n，使得 $ne=0$，则满足这条件的最小正整数 n 叫作域 F 的**特征**. 如果不存在正整数 n 使得 $ne=0$，则称域 F 的特征为零.

例如有理数域，实数域和复数域的特征均为零，因为这些域的幺元素就是数 1，而对每个正整数 $n, n\cdot e=n\cdot 1=n$ 不为零. 又如 p 元域 F_p 的特征是 p，因为 F_p 的幺元素为[1]，零元素为[0]，而 $p\cdot[1]=[1]+[1]+\cdots+[1]=[p]=[0]$，并且 p 是使此式成立的最小正整数.

1.2.5 定理 域的特征或者为零，或者为素数.

证明 若域 F 的特征不为零，则存在正整数 n，使得 $ne=0$. 设 n 是满足此条件的最小正整数，即 n 为 F 的特征. 由于 $e\neq 0$，从而 $n\neq 1$，即 $n\geqslant 2$. 如果 n 不是素数，则 n 可写成两个比 n 小的正整数之积：$n=n_1\cdot n_2, 1\leqslant n_1, n_2<n$. 于是

$$(n_1e)(n_2e) = n_1n_2e^2 = ne = 0.$$

从而 $n_1e=0$ 或者 $n_2e=0$. 但这与 n 的最小性相矛盾. 所以 n 必为素数.

注记 若域 F 的特征为零，则对于不同的整数 n 和 m，ne 与 me 是 F 中不同的元素.(因为若 $ne=me$，而 $n\neq m$，不妨设 $n>m$，则 $n-m$ 为正整数，而 $(n-m)e=ne-me=0$，这与 F 的特征为零相矛盾.)于是 F 有子集合

$$A = \{0 = 0\cdot e, \pm 1e, \pm 2e, \pm 3e, \cdots\}.$$

将 A 中元素 ne 对应成整数 n，这是 A 与整数环 $\mathbf{Z}$ 之间的一一对应. 如果再考虑这两个集合的代数结构，即考虑 A 和 $\mathbf{Z}$ 中的运

算，则上述对应与加法和乘法运算是相协调的，即 ne 与 me 之和 $(n+m)e$ 恰好对应于 n 与 m 之和 $n+m$，而 ne 与 me 之积 $(ne)(me)=(nm)e$ 恰好对应于 n 与 m 之积 nm. 所以我们可以把 A 等同于整数环 $\mathbf{Z}$，在这种等同之下，e 写成 1，ne 写成 n. 进而，若 n 和 m 是整数，$m\neq 0$. 则 $me\neq 0$，于是 F 中有元素 $\frac{ne}{me}$，我们把它写成 $\frac{n}{m}$，即看成是有理数，从而**每个特征零的域都以有理数域作为子域**. 特别地，每个特征零的域都是无限域，或者换句话说，**有限域的特征一定是素数**.

若 K 是域 F 的子域，则 K 和 F 的特征是相同的，因为它们有公共的幺元素 e，而域的特征的定义只与 e 有关. 特别地，有理函数域 $\mathbf{F}_p(x)$ 的特征与 p 元域 $\mathbf{F}_p$ 的特征一样，都是素数 p. 这个例子也表明，无限域的特征不一定为零，也可以是素数.

设域 F 的特征为素数 p. 则 $0=0e,1e,2e,\cdots,(p-1)e$ 是 F 中 p 个不同的元素，而 $pe=0$. 如果将 F 中元素 ne 看成是 $\mathbf{F}_p$ 中元素 $[n]$ $(0\leqslant n\leqslant p-1)$. 那末 $\mathbf{F}_p$ 成为 F 的子域. 综合上述，可知有理数域和 p 元域 $\mathbf{F}_p$ 是一批最小的域. 每个域或者包含有理数域（当特征为零时），或者包含某个 p 元域 $\mathbf{F}_p$（当特征为 p 时）.

由于本书主要对象为有限域，所以请大家要特别注意特征 p 域的性质. 下面是其中的一些.

1.2.6 定理 设域 F 的特征为素数 p，e 为域 F 的幺元素，则

(1) 对每个 $a\in F$，$a+a+\cdots+a$（p 个）$=pa=0$.

(2) 若 m 为整数，$a\neq 0$，则 $ma=0\Longleftrightarrow p\mid m$.

(3) 对于 $a,b\in F$ 和每个正整数 n，

$$(a+b)^{p^n}=a^{p^n}+b^{p^n}.$$

(4) 对每个正整数 n，集合

$$F^{p^n}=\{a^{p^n}|a\in F\}$$

是 F 的子域.

证明 (1) $a+a+\cdots+a=a\cdot e+ae+\cdots+ae$

$$=a(e+e+\cdots+e)$$

$$=a(pe)=a\cdot 0=0.$$

(2)若 $p|m$，则$\frac{m}{p}\in\mathbf{Z}$. 而 $ma=\frac{m}{p}(pa)=\frac{m}{p}\cdot 0=0$. 若 $ma=0$. 由除法算式，$m=qp+r$，其中 $q,r\in\mathbf{Z}$，$0\leqslant r\leqslant p-1$. 于是 $ra=(m-qp)a=ma-q(pa)=0-0=0$. 从而必然 $r=0$，即 $p|m$.

(3)可象定理 1.1.7 一样证得$(a+b)^p=a^p+b^p$. 然后$(a+b)^{p^n}=(a^p+b^p)^{p^{n-1}}=(a^{p^2}+b^{p^2})^{p^{n-2}}=\cdots=a^{p^n}+b^{p^n}$.

(4)对于 F^{p^n}中元素 a^{p^n}和 b^{p^n}，$a^{p^n}+b^{p^n}=(a+b)^{p^n}$和 $a^{p^n}b^{p^n}=(ab)^{p^n}$均是 F^{p^n}中元素，又$(a^{p^n})^{-1}=(a^{-1})^{p^n}$(当 $a\neq 0$ 时)，$-a^{p^n}=(-a)^{p^n}$(当 p 为奇素数时，$(-a)^{p^n}=(-1)^{p^n}\cdot a^{p^n}=-a^{p^n}$，当 F 的特征 p 等于 2 时，$2a=0$，从而 $a=-a$，于是又有$(-a)^{p^n}=a^{p^n}=-a^{p^n}$). 于是 F^{p^n}为 F 的子域.

注记 F^{p^n}可以为 F 的真子域，也可以等于 F. 例如 $F=\mathbf{F}_p$ 时，$\mathbf{F}_p^p=\{a^p\,|\,a\in\mathbf{F}^p\}$，但是对 $\mathbf{F}_p$ 中每个元素 a，$a^p=a$(定理 1.1.8). 所以 $\mathbf{F}_p^p=\{a|a\in\mathbf{F}_p\}=\mathbf{F}_p$. 于是对每个正整数 n，$\mathbf{F}_p^{p^n}=\mathbf{F}_p$. 若 F 为有理函数域 $\mathbf{F}_p(x)$. 对于每个多项式 $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n(a_i\in\mathbf{F}_p)$，则 $f(x)^p=(a_0x^n+a_1x^{n-1}+\cdots+a_n)^p=(a_0x^n)^p+(a_1x^{n-1})^p+\cdots+a_n^p=a_0^px^{np}+a_1^px^{(n-1)p}+\cdots+a_n^p=a_0(x^p)^n+a_1(x^p)^{n-1}+\cdots+a_n=f(x^p)$. 从而对每个有理函数$\frac{f(x)}{g(x)}$(其中 $f(x),g(x)\in\mathbf{F}_p[x]$，$g(x)\neq 0$)，$\left(\frac{f(x)}{g(x)}\right)^p=\frac{f(x)^p}{g(x)^p}=$

$\frac{f(x^p)}{g(x^p)}$. 这就表明$(\boldsymbol{F}_p(x))^p=\boldsymbol{F}_p(x^p)$. 于是对每个正整数 n, $(\boldsymbol{F}_p(x))^{p^n}=\boldsymbol{F}_p(x^{p^n})$. 而这是 $\boldsymbol{F}_p(x)$的真子域.

1.2.7 习 题

1. 补足定理 1.2.2 的证明，并且证明其后的(7)，(8)，(9).
2. 下列集合哪些是复数域的子域？

   (Ⅰ)$\{a+bi\mid a$ 和 b 是整数$\}$，$i=\sqrt{-1}$.

   (Ⅱ)$\{a+bi\mid a$ 和 b 是有理数$\}$

   (Ⅲ)$\{a+b\sqrt[3]{2}+c\sqrt[3]{4}\mid a,b,c$ 是有理数$\}$.
3. 设域 F 的特征为素数 p，$a\in F$. 求证方程 $x^p=a$ 在 F 中最多有一个解.
4. 设 F 为域，$g\in F$. 如果 F 中每个非零元素均可表示成 $g^n(n\in \boldsymbol{Z})$，则 F 必为有限域.
5. 设 $f(x)\in \boldsymbol{F}_p[x]$. a 是 $\boldsymbol{F}_p$ 的某个扩域中的元素. 如果 a 是多项式 $f(x)$的根(即 $f(a)=0$)，则对每个正整数 n，a^{p^n} 也是 $f(x)$的根.

§1.3 域上的多项式

大家在中学里学习过系数为有理数、实数或复数的多项式之间的运算和多项式的许多性质. 事实上，有许多性质在多项式系数属于任意域时也仍然有效. 在这一节里我们谈谈任意域上多项式的一般性质. 我们也需注意某些域(尤其是特征 p 的域)上多项式的特殊性质.

设 F 为任意域. 和上一节一样，我们用 $F[x]$表示系数属于 F 的所有多项式构成的集合. 我们把 $F[x]$ 叫成多项式环，因

$F[x]$对于自然定义的加法和乘法运算，满足域的定义 1.2.1 中除了（Ⅰ.4）之外的所有其他公理.

对于 $F[x]$中每个多项式

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n, \quad (a_i \in F)$$

若 $a_0 \neq 0$，称 $f(x)$为 n 次多项式，并且用 $\deg f$ 表示 $f(x)$的次数. 如果首项系数 a_0 是 1，则 $f(x)$叫作首 1 多项式. 若 α 是 F 的某个扩域 E 中的元素，则

$$f(\alpha) = a_0\alpha^n + a_1\alpha^{n-1} + \cdots + a_n$$

是 E 中的元素，叫作 $f(x)$在 α 处的取值. 如果 $f(\alpha)=0$，则称 α 是 $f(x)$在 E 中的一个根. 大家在中学里学过，一个 n 次方程最多有 n 个根. 这件事对任意域 F 的情况也是对的，并且证明也和中学里完全一样，其基本工具是多项式环 $F[x]$中的除法算式.

设 $f(x)$和 $g(x)$均是 $F[x]$中多项式，其中

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n, \quad a_0\neq 0, \deg f=n.$$

$$g(x)=b_0x^m+b_1x^{m-1}+\cdots+b_m, \quad b_0\neq 0, \deg g=m\geqslant 1.$$

我们用 $g(x)$去除 $f(x)$. 如果 $n\geqslant m$，我们得到商 $a_0b_0^{-1}x^{n-m}$，然后从 $f(x)$中减去 $b_0^{-1}x^{n-m}g(x)$，剩下多项式为

$$\begin{aligned} f_1(x) &= f(x)-b_0^{-1}x^{n-m}g(x) \\ &= (a_0x^n+a_1x^{n-1}+\cdots)-a_0b_0^{-1}x^{n-m}(b_0x^m+b_1x^{m-1}+\cdots) \\ &= (a_1-a_0b_0^{-1}b_1)x^{n-1}+\cdots \end{aligned}$$

于是 $\deg f_1<\deg f=n$. 如果仍然 $\deg f_1\geqslant m$，再这样进行下去. 最后剩下一个次数 $<m$ 的多项式 $r(x)$作为余式，而把逐次商加起来就是总的商式 $q(x)$，就得到下面的除法算式

$$f(x) = q(x)g(x) + r(x). \qquad (*)$$

其中 $q(x), r(x)\in F[x]$，$r(x)=0$，或者 $\deg r(x)<\deg g(x)$.

例如用 $q(x)=2x^2+7$ 去除 $f(x)=x^3+x^2+7$. 如果系数属于有理数域,便得到下面的除法算式

$$
\begin{array}{r}
\frac{1}{2}x+\frac{1}{2} \qquad\quad \\
2x^2+7\overline{\big)\, x^3+x^2 \qquad\qquad +7} \\
\underline{x^3+\qquad \frac{7}{2}x \qquad\quad} \\
x^2-\frac{7}{2}x+7 \\
\underline{x^2 \qquad\qquad +\frac{7}{2}} \\
-\frac{7}{2}x+\frac{7}{2}
\end{array}
$$

即 $x^3+x^2+7=\left(\frac{1}{2}x+\frac{1}{2}\right)(2x^2+7)+\left(-\frac{7}{2}x+\frac{7}{2}\right)$.

如果在 $F_{11}[x]$ 中,那末除法算式为

$$
\begin{array}{r}
6x+6 \qquad \\
2x^2+7\overline{\big)\, x^3+x^2 \qquad +7} \\
\underline{x^3 \qquad +9x \qquad} \\
x^2+2x+7 \\
\underline{x^2 \qquad\quad +9} \\
2x+9
\end{array}
$$

即在 $F_{11}[x]$ 中的除法算式为

$$x^3+x^2+7=(6x+6)(2x^2+7)+(2x+9).$$

1.3.1 定义 设 F 为域,$f(x),g(x)\in F[x]$,$g(x)\neq 0$. 如果存在多项式 $q(x)\in F[x]$,使得 $f(x)=q(x)g(x)$(这也相当于除法算式(*)中余式 $r(x)$ 为 0),则称 $g(x)$**整除** $f(x)$,表示成

$g(x)|f(x)$. 否则便称 $g(x)$ 不能整除 $f(x)$，表示成 $g(x)\nmid f(x)$.

多项式的整除和整数的整除有许多类似的性质. 例如：若 $g(x)|f(x)$，$f(x)|h(x)$，则 $g(x)|h(x)$. 又如：若 $g(x)|f(x)$，$g(x)|h(x)$，则 $g(x)|f(x)\pm h(x)$ 等等.

1.3.2 定理 设 F 为域，$f(x)\in F[x]$. c 属于 F 的某个扩域 E（于是 $x-c\in E[x]$，而 $f(x)$ 也可看成是 $E[x]$ 中的多项式），则

$$c \text{ 为 } f(x) \text{ 的根} \iff \text{在 } E[x] \text{ 中 } (x-c)|f(x).$$

证明 在 $E[x]$ 中用 $x-c$ 去除 $f(x)$，余式的次数小于 1，从而余式为 E 中元素，即除法算式为：

$$f(x)=q(x)(x-c)+a,\ q(x)\in E[x], a\in E.$$

将 $x=c$ 代入此式，得到 $f(c)=q(c)(c-c)+a=a$. 因此

$$f(x)=q(x)(x-c)+f(c).$$

于是：c 为 $f(x)$ 的根 $\iff f(c)=0 \iff f(x)=q(x)(x-c)$

$$\iff (x-c)|f(x).$$

1.3.3 定理 设 F 为域，$f(x)$ 为 $F[x]$ 中非零多项式. $n=\deg f$. 则 $f(x)$ 在 F 的任意扩域 E 中相异根的个数不超过 n.

证明 设 c_1 为 $f(x)$ 的根，$c_1\in E$. 由定理 1.3.2 知有 $q(x)\in E[x]$，使得 $f(x)=q(x)(x-c_1)$. 如果 E 中元素 c_2 是 $f(x)$ 的另一个根，即 $c_1\neq c_2$. 则 $0=f(c_2)=q(c_2)(c_2-c_1)$. 由 $c_2-c_1\neq 0$ 可知 $q(c_2)=0$，即存在多项式 $h(x)$，使得 $g(x)=h(x)(x-c_2)$. 于是 $f(x)=h(x)(x-c_1)(x-c_2)$. 这样下去，若 $c_1,\cdots,c_m$ 是 E 中彼此不同的元素，并且它们均是 $f(x)$ 的根，则可得到 $f(x)=l(x)(x-c_1)(x-c_2)\cdots(x-c_m)$，其中 $l(x)\in E[x]$. 于是

$m=\deg(x-c_1)\cdots(x-c_m)\leqslant\deg f(x)=n$. 即 $f(x)$在 E 中存在至多 n 个不同的根.

注记 以 A 表示模 8 的同余类构成的集合$\{0,1,2,\cdots,7\}$(这是一个环). 则多项式 x^2-1 在 A 中有四个根:1,3,5,7. 这表明定理 1.3.3 中 F 和 E 为域的条件是不可缺少的.

多项式环 $F[x]$与整数环有相似的性质:它们都有除法算式(虽然具体形式不同),也都有整除概念. 事实上,它们还有许多相似之处. 例如对应于素数,在 $F[x]$中有下面的不可约多项式概念,以下 F 总表示是一个域.

1.3.4. 定义 设 $f(x),g(x)\in F[x]$. 如果 $g(x)\mid f(x)$,称 $g(x)$为 $f(x)$的**因式**或**因子**,而 $f(x)$为 $g(x)$的**倍式**. 设 $\deg f\geqslant 1$. 如果 $f(x)$不能写成 $F[x]$中两个次数小于 $\deg f$ 的多项式之乘积,则称 $f(x)$为 $F[x]$中**不可约多项式**,换句话说,

$f(x)$为 $F[x]$中不可约多项式

$\Longleftrightarrow f(x)$在 $F[x]$中的因子只有 a 或 $af(x)$

(其中 a 为 F 中非零元素)

$\Longleftrightarrow f(x)$在 $F[x]$中的首 1 多项式因子只有 1 和 $f(x)$自身.

若 $f(x)$和 $g(x)$在 $F[x]$中的首 1 多项式公因子只有 1,则称 $f(x)$和 $g(x)$在 $F[x]$中**互素**.

例如:$F[x]$中所有一次多项式 $ax+b(a,b\in F,a\neq 0)$都是不可约的. 如果 $f(x)$是 $F[x]$中不可约多项式,则 $f(x)$的首 1 多项式因子只有 1 和 $f(x)$自身. 从而当 $f(x)\nmid g(x)$时,$f(x)$和 $g(x)$的首 1 多项式公因子只有 1,即 $f(x)$和 $g(x)$互素.

下面一条定理很象定理 1.1.3,并且连证明也是一样的.

1.3.5 定理 设 $f(x)$和 $g(x)$是 $F[x]$中互素的多项式. 则存在 $A(x),B(x)\in F[x]$使得 $A(x)f(x)+B(x)g(x)=1$.

证明 考虑集合

$$S=\{Af+Bg \mid A,B\in F[x]\}.$$

我们只需证明 $1\in S$,可以象定理 1.1.3 证明中那样,得到集合 S 具有下列性质:

(1) 若 $h(x),h'(x)\in S$,则 $h(x)\pm h'(x)\in S$.

(2) 若 $h(x)\in S$,则对 $F[x]$中每个多项式 $l(x)$,$h(x)l(x)\in S$.

由于 f 和 g 不全为零(否则便不会互素),又易知 $f\in S$,$g\in S$. 从而 S 中包含非零多项式. 由(2)即知 S 中必包含首 1 多项式. 我们在 S 中取一个次数最小的首 1 多项式 $l(x)$. 则

(3) S 中每个多项式都是 $l(x)$的倍式.

为证(3),我们仍利用除法算式. 设 $h(x)\in S$,则有除法算式 $h(x)=q(x)l(x)+r(x)$,其中 $q(x),r(x)\in F[x]$,$r(x)$或者为零,或者 $\deg r(x)<\deg l(x)$. 由(1)和(2)可知 $r(x)=h(x)-q(x)l(x)\in S$. 再由 $l(x)$在 S 中次数的最小性知 $r(x)$必然为零,于是 $l(x)\mid h(x)$.

由于 $f\in S$,$g\in S$,再由(3)可知 $l(x)$是 f 和 g 的首 1 多项式公因子,由 f 和 g 互素即知 $l(x)=1$,于是 $1\in S$,这就完成了定理 1.3.5 的证明.

1.3.6 定理 设 $p(x)$是 $F[x]$中不可约多项式. 如果 $A(x),B(x)\in F[x]$,$p(x)\mid A(x)B(x)$,则 $p(x)\mid A(x)$或者 $p(x)\mid B(x)$.

证明 若 $p(x)\nmid A(x)$,则 $p(x)$与 $A(x)$互素,于是有 $g(x)$,$h(x)\in F[x]$,使得 $p(x)g(x)+A(x)h(x)=1$(定理 1.3.5). 从

而 $p(x)|p(x)(g(x)B(x))+(A(x)B(x))h(x)=B(x)$.

整数环 Z 的最基本性质是每个大于 1 的正整数均可唯一表示成有限个素数之积. 有了上述准备，我们可证明多项式环 $F[x]$ 中类似性质.

1.3.7 定理 （多项式环 $F[x]$ 的唯一因式分解性质）. $F[x]$ 中每个次数 $\geqslant 1$ 的首 1 多项式 $f(x)$ 均可表成有限个首 1 不可约多项式之积，

$$f(x)=p_1(x)p_2(x)\cdots p_s(x), \qquad (*)$$

其中 $p_i(x)(1\leqslant i\leqslant s)$ 均为 $F[x]$ 中首 1 不可约多项式，$s\geqslant 1$. 并且这个表达式不计因子 $p_i(x)$ 的次序是唯一的.

证明 先证明分解式（*）的存在性. 若 $f(x)$ 不可约，则 $f(x)=f(x)$ 就是分解式（$s=1$）. 否则，$f(x)=g_1(x)g_2(x)$，其中 $g_1(x)$ 和 $g_2(x)$ 均是 $F[x]$ 中次数小于 $\deg f$ 的首 1 多项式. 然后我们对多项式的次数作数学归纳法，由 $g_1(x)$ 和 $g_2(x)$ 都有形如（*）的分解式就得到 $f(x)$ 的分解式.

现在证分解式（*）的唯一性，若又有

$$f(x) = q_1(x)\cdots q_n(x),$$

其中 $n\geqslant 1$，$q_i(x)$ 均为 $F[x]$ 中首 1 不可约多项式. 则 $p_1(x)\cdots p_s(x)=q_1(x)\cdots q_n(x)$. 于是 $p_1(x)|q_1(x)\cdots q_n(x)$. 由定理 1.3.5 可知 $p_1(x)$ 必可整除某个 $q_i(x)$. 适当调整 $q_i(x)$ 的次序，不妨设 $p_1(x)|q_1(x)$. 由于 $p_1(x)$ 和 $q_1(x)$ 均是首 1 不可约多项式，必然 $p_1(x)=q_1(x)$. 于是 $p_2(x)\cdots p_s(x)=q_2(x)\cdots q_n(x)$. 继续下去，即知 $s=n$，并且（适当调整 $q_i(x)$ 的次序之后）$p_i(x)=q_i(x)(1\leqslant i\leqslant s)$.

和整数环 Z 的情形一样，定理 1.3.7 所述的唯一因式分解

特性也是多项式环$F[x]$的很基本性质．由它可以衍生出许多概念和结论．

例如：若$f(x)$是$F[x]$中次数$\geqslant 1$的多项式，则由定理1.3.7可知，$f(x)$可唯一表达成

$$f(x)=a\cdot p_1(x)\cdots p_s(x),$$

其中a为$f(x)$的首项系数，$p_i(x)(1\leqslant i\leqslant s)$均是$F[x]$中首1不可约多项式，所以$f(x)$在$F[x]$中的首1多项式因子只能是1或者一部份$p_i(x)$的乘积，即$f(x)$只有有限多个首1多项式因子．当$f(x)$和$g(x)$是$F[x]$中不全为零的两个多项式，那末它们的首1多项式公因子也只有有限多个．设$h(x)$是它们的一个次数最大的首1多项式公因子．可以证明：集合$S=\{f(x)A(x)+g(x)B(x)\mid A(x),B(x)\in F[x]\}$恰好是$h(x)$的所有倍式构成的集合．（仿照定理1.1.3的证明）．因此$h(x)$是由$f(x)$和$g(x)$所唯一决定的．我们将$h(x)$叫作$f(x)$和$g(x)$的**最大公因子**，表示成$(f(x),g(x))$．多项式的最大公因子也有与定理1.1.4相仿的一些性质．我们把这些性质的确切叙述和证明留给读者．

仍设$f(x)$是$F[x]$中次数$\geqslant 1$的多项式．则对于F的某个扩域E和E中元素α，α为$f(x)$的根的充要条件为在$E[x]$中$(x-\alpha)\mid f(x)$（定理1.3.2）．设多项式$f(x)$在$E[x]$中分解成

$$f(x)=a\cdot p_1(x)\cdots p_s(x),$$

其中a为$f(x)$的首项系数，$p_i(x)$为$E[x]$中首1不可约多项式．如果$p_i(x)(1\leqslant i\leqslant s)$当中恰好有$m$个是$(x-\alpha)$，则$(x-\alpha)^m\mid f(x)$，而$(x-\alpha)^{m+1}\nmid f(x)$．当$m\geqslant 2$时，称$\alpha$是$f(x)$的**重根**．

现在我们准备给出判别一个多项式何时有重根的简单法则，首先我们需要

1.3.8 引理 设 $f(x),g(x)\in F[x]$，E 为 F 的扩域. 则：$f(x)$ 和 $g(x)$ 在 $F[x]$ 中互素 $\Longleftrightarrow f(x)$ 和 $g(x)$ 在 $E[x]$ 中互素.

证明 若 $f(x)$ 和 $g(x)$ 在 $E[x]$ 中互素，由定义即知 $f(x)$ 和 $g(x)$ 在 $F[x]$ 中也互素. 反之，若 $f(x)$ 和 $g(x)$ 在 $F[x]$ 中互素，则有 $A(x),B(x)\in F[x]$ 使得 $f(x)A(x)+g(x)B(x)=1$. 设 $f(x)$ 和 $g(x)$ 在 $E[x]$ 中有首 1 多项式公因子 $h(x)$，则 $h(x)\mid f(x)A(x)+g(x)B(x)=1$. 于是 $h(x)=1$. 这就表明 $f(x)$ 和 $g(x)$ 在 $E[x]$ 中也互素.

1.3.9 定义 设 $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$ 为 $F[x]$ 中多项式. 我们把 $F[x]$ 中多项式

$$f'(x)=na_0x^{n-1}+(n-1)a_1x^{n-2}+\cdots+a_{n-1}$$

叫作 $f(x)$ 的**形式微商**.

这个名词来源于微积分学. 如果 F 为复数域，即 $f(x)$ 是复系数多项式，则 $f'(x)$ 就是通常所说的 $f(x)$ 的微商. 我们可以用定义直接验证，对于任意域 F，形式微商也满足通常求微商的下列法则(请读者自行验证，因为只涉及代数恒等式的验证).

(i) $(f\pm g)'=f'\pm g'$，$(cf)'=cf'$ (对于 $c\in F$).

(ii) $(fg)'=f'g+fg'$，$(f^n)'=n(f)^{n-1}f'$ (对于 $n\geqslant 1$).

但是我们还是要注意一个区别. 当 F 为复数域以及任意特征为零的域时，若 $f(x)$ 为 n 次多项式. ($n\geqslant 1$)，则 $f'(x)$ 必为 $n-1$ 次多项式(因为若 $f(x)=a_0x^n+\cdots$ 的首项系数 $a_0\neq 0$，则 $f'(x)=na_0x^{n-1}+\cdots$ 的首项系数 na_0 也不为零). 但是对特征为素数 p 的域则不然，例如在 $F_p(x)$ 中 $f(x)=x^p-1$ 是 p 次多项式，但是 $f'(x)=px^{p-1}=0\cdot x^{p-1}=0$. 其原因在于，$x^p$ 指数上的 p 看成是通常正整数，而微商之后落到系数中则成了 F_p 中元素！

1.3.10 定理 （重根判别法）设 $f(x)$ 为 $F[x]$ 中的多项式. $\deg f\geqslant 1$. c 为 F 的某个扩域 E 中的元素，则

(1) c 为 $f(x)$ 的重根 $\Longleftrightarrow f(c)=f'(c)=0$.

(2) $f(x)$ 在 F 的任意扩域中均没有重根 $\Longleftrightarrow f(x)$ 和 $f'(x)$ 在 $F[x]$ 中互素.

证明 (1)设 c 为 $f(x)$ 的重根，则 $f(x)=(x-c)^2\cdot g(x)$，其中 $g(x)\in E[x]$. 于是 $f'(x)=((x-c)^2)'g(x)+(x-c)^2\cdot g'(x)=2(x-c)g(x)+(x-c)^2g'(x)$. 从而 $f(c)=f'(c)=0$. 反之若 $f(c)=0$，则 $f(x)=(x-c)g(x)$. 于是 $f'(x)=g(x)+(x-c)\cdot g'(x)$. 如果又有 $f'(c)=0$，则 $0=f'(c)=g(c)+(c-c)\cdot g'(c)=g(c)$. 从而 $(x-c)\mid g(x)$，于是 $(x-c)^2\mid f(x)$，即 c 为 $f(x)$ 的重根.

(2) 若 c 是 $f(x)$ 的重根，c 属于 F 的某个扩域. 从而 $f(c)=f'(c)=0$（由(1)）. 因此在 $E[x]$ 中 $(x-c)$ 是 $f(x)$ 和 $f'(x)$ 的公因子. 从而 f 和 f' 在 $E[x]$ 中不互素. 由引理 1.3.9 知 f 和 f' 在 $F[x]$ 中也不互素. 反之，若 f 和 f' 在 $F[x]$ 中不互素，则它们有公因子 $h(x)$，其中 $h(x)$ 为 $F[x]$ 中次数 $\geqslant 1$ 的多项式. 下面的注记表明 $h(x)$ 必在 F 的某个扩域 E 中有根 α. 于是 $h(\alpha)=0$，由于 $h(x)\mid f(x)$，$h(x)\mid f'(x)$，从而 $f(\alpha)=f'(\alpha)=0$. 因此 α 是 $f(x)$ 的重根.

注记 我们从中学里知道，每个次数大于等于 1 的实系数多项式在复数域中必有根. 现在我们要问：对于任意域 F，$F[x]$ 中任意次数 $\geqslant 1$ 的多项式 $f(x)$ 是否在 F 的某个扩域 E 中有根？答案也是肯定的. 现在我们简要地谈谈如何构作扩域 E. 首先，$f(x)$ 是一些不可约多项式之积，而每个不可约因子的根也是 $f(x)$ 的根. 所以我们不妨假定 $f(x)$ 是 $F[x]$ 中的首 1 不可约多

项式.

$F[x]$中两个多项式 $A(x)$ 和 $B(x)$ 叫作模 $f(x)$ 同余，是指 $f(x)\mid A(x)-B(x)$. 我们以$[A(x)]$表示与 $A(x)$ 模 f 同余的所有多项式组成的集合，叫作模 f 的一个同余类. 我们以 S 表示所有模 f 同余类构成的集合，并且在 S 中自然定义加法和乘法：

$$[A(x)]+[B(x)]=[A(x)+B(x)],$$
$$[A(x)][B(x)]=[A(x)B(x)].$$

可以证明 S 由此成为域. 这里的关键又在于要验证域定义 1.2.1中的公理(Ⅰ.4)，利用 $f(x)$ 不可约和定理 1.3.5 即可验证公理(Ⅰ.4)的正确性. 整个情形与验证整数环 $\mathbf{Z}$ 模 p 同余类全体形成域是完全一样的.

域 F 中每个元素 a 等同于 S 中元素$[a]$，于是 F 可看成是 S 的一个子域. 即 S 为 F 的扩域. 将 S 中元素$[x]$代到 $f(x)$ 中：

$$\begin{aligned}f([x])&=a_0[x]^n+a_1[x]^{n-1}+\cdots+a_n\\&=[a_0x^n+a_1x^{n-1}+\cdots+a_n]\\&=[f(x)]=[0].\end{aligned}$$

这就表明 $f(x)$ 在 F 的扩域 S 中有根$[x]$. 从而完成了证明.

设 $f(x)$ 为 $F[x]$中首 1n 次多项式，$n\geqslant 1$. 由此所述，$f(x)$ 在 F 的某个扩域 E 中有根 α_1. 从而 $f(x)=(x-\alpha_1)\cdot g(x)$，其中 $g(x)$ 为 $E[x]$中的 $n-1$ 次多项式. 如果 $n-1\geqslant 1$，则 $g(x)$ 又在 E 的某个扩域 K 中有根 α_2，于是 $g(x)=(x-\alpha_2)h(x)$，而 $f(x)=(x-\alpha_1)(x-\alpha_2)h(x)$，如此进行有限步之后，我们得到 F 的充分大的扩域 M，使得 $f(x)$ 可以写成

$$f(x)=(x-\alpha_1)\cdots(x-\alpha_n),$$

从而 n 次多项式(在 F 的某个扩域中)恰好有 n 个根，不过有些根可能相同，从而要考虑重数.

若将 $F[x]$ 中所有多项式的所有根都加在 F 中而造成一个非常大的扩域 K(这是非常不确切的用词!)则 $F[x]$ 中每个多项式的根都在 K 中,我们把 K 叫作 F 的**代数闭包**.通常我们总是固定 F 的一个代数闭包 K,使得 $F[x]$ 中每个多项式的根都看成是 K 中元素.

1.3.11 习　题

(以下 F 均为域)

1. 设 $f(x)$ 和 $g(x)$ 为 $F[x]$ 中多项式.

   (Ⅰ) 若 $f(x)$ 和 $g(x)$ 均不为零,则

   $\deg(f+g)\leqslant\max(\deg f,\deg g)$

   $\deg(fg)=\deg f+\deg g$.

   (Ⅱ) 若 $fg=0$,则 $f=0$ 或者 $g=0$.

2. 设 $f(x),g(x)\in F[x]$,$g(x)\neq 0$,$f(x)=q(x)g(x)+r(x)$ 为除法算式,其中 $q(x),r(x)\in F[x]$,$r(x)=0$ 或者 $\deg r(x)<\deg g(x)$.求证多项式 $q(x)$ 和 $r(x)$ 均由 f 和 g 所唯一决定.

3. 列出 $F_2[x]$ 和 $F_3[x]$ 中所有三次不可约首 1 多项式.

4. 将 $F_2[x]$ 中多项式 x^7+1 和 $x^{10}+1$ 分解成 $F_2[x]$ 中不可约多项式之积.

5. 设 F 的特征为素数 p. $f(x)$ 为 $F[x]$ 中首 1 不可约多项式.求证:$f(x)$ 在 F 的某个扩域中有重根 $\Longleftrightarrow f(x)$ 是 x^p 的多项式.

6. 设 p 为素数,求证 $F_p[x]$ 中不可约多项式在 F_p 的每个扩域中均没有重根.

§1.4 有　限　域

有了前三节的准备,现在可以研究任意有限域.首先,对于

有限域的元素个数有如下限制

1.4.1 定理 有限域的元素个数必为 p^n,其中 p 为素数,$n\geqslant 1$.

证明 有限域 F 的特征必为素数 p,于是 $\mathbf{F}_p$ 为 F 的子域(见定理 1.2.5 后面的注记).

我们把 F 的一个子集 $\{x_1,\cdots,x_n\}$ 叫作生成集,是指 F 中每个元素 x 均可表成

$$x = a_1x_1 + \cdots + a_nx_n, \qquad (1)$$

其中 $a_i\in\mathbf{F}_p(1\leqslant i\leqslant n)$,$F$ 本身显然是 F 的一个生成集.在所有的生成集中取其中包含元素最少的一个,仍记为 $\{x_1,\cdots,x_n\}$,则 F 中每个元素 x 均可用 $x_1,\cdots,x_n$ 表示成(1)式形式.现在我们证明对每个 $x\in F$,表达式(1)是唯一的.因为若又有

$$x = b_1x_1 + \cdots + b_nx_n \qquad (b_i \in \mathbf{F}_p),$$

则 $(a_1-b_1)x_1+\cdots+(a_n-b_n)x_n=0$.如果有某个 a_i-b_i 不为零,不妨设 $a_n-b_n\neq 0$,则

$$x_n=\frac{-1}{a_n-b_n}((a_1-b_1)x_1+\cdots+(a_{n-1}-b_{n-1})x_{n-1}). \quad (2)$$

即 x_n 可以用 $x_1,\cdots,x_{n-1}$ 表示(系数仍属于 $\mathbf{F}_p$).由于 F 中每个元素 x 均可用 $x_1,\cdots,x_n$ 表示,将(2)式代入表达式中,可知 x 可用 $x_1,\cdots,x_{n-1}$ 表示.这表明 $\{x_1,\cdots,x_{n-1}\}$ 是生成组,与生成组 $\{x_1,\cdots,x_n\}$ 元素最少相矛盾.所以 $a_i-b_i=0$,即 $a_i=b_i$(对每个 $i,1\leqslant i\leqslant n$).从而表达式(1)是唯一的.

于是,在(1)式中 $a_1,\cdots,a_n$ 分别取 $\mathbf{F}_p$ 中的 p 个元素,共有 p^n 种取法.由上述知不同的取法给出 F 中不同的元素,并且由此得到 F 的全部元素,从而 F 中共有 p^n 个元素.

注记 对于熟悉线性代数的人,定理 1.4.1 的证明可以只

用一行字：F 为 $\mathbf{F}_p$ 上向量空间．由于 F 有限，从而 F 在 $\mathbf{F}_p$ 上的维数有限，设维数是 n，则 F 有 p^n 个元素．证明中所谓"元素个数最少的生成组"即指 $\mathbf{F}_p$-向量空间 F 的一组基．

现在我们证明，对每个素数幂 p^n 均存在 p^n 元有限域．

1.4.2　定理　设 p 为素数，$n\geqslant 1$．Ω_p 为 $\mathbf{F}_p$ 的代数闭包．则多项式 $x^{p^n}-x$ 在 Ω_p 中的所有根形成 p^n 元有限域．

证明　我们在上节末尾的注记中说过，$f(x)=x^{p^n}-x$ 在 $\mathbf{F}_p$ 的代数闭包 Ω_p 中共有 p^n 个根．由于 $f'(x)=p^n\cdot x^{p^n-1}-1=-1$，即 $(f,f')=1$．从而 $x^{p^n}-x$ 没有重根（定理 1.3.10）．以 S 表示这 p^n 个不同的根构成的集合．它是域 Ω_p 的 p^n 元子集．为证 S 是域，我们只需验证：

（1）若 $a,b\in S$，则 $-a\in S$，$a+b\in S$，$ab\in S$．

（2）若 $a\in S$，$a\neq 0$，则 $a^{-1}\in S$．

若 $a,b\in S$，则 $a^{p^n}=a$，$b^{p^n}=b$，于是 $(a+b)^{p^n}=a^{p^n}+b^{p^n}=a+b$，$(ab)^{p^n}=a^{p^n}b^{p^n}=ab$，从而 $a+b,ab\in S$．又当 p 为奇素数时，$(-a)^{p^n}=(-1)^{p^n}a^{p^n}=-a$，而当 $p=2$ 时，$-a=a$．从而总有 $-a\in S$．最后若 $a\neq 0$，则 $(a^{-1})^{p^n}=(a^{p^n})^{-1}=a^{-1}$．从而 $a^{-1}\in S$．这就证明了 S 为 p^n 元有限域．

定理 1.4.2 解决了 p^n 元有限域的存在性问题．现在解决唯一性问题．

1.4.3　定理　设 Ω_p 为 $\mathbf{F}_p$ 的代数闭包，则对每个 $n\geqslant 1$，Ω_p 中恰好有一个 p^n 元有限域．

证明　记 $q=p^n$．设 F 是 Ω_p 的一个 p^n 元子域．F 的非零元素为 $x_1,\cdots,x_{q-1}$，对于 F 的每个非零元素 a，易知 $ax_1,\cdots,ax_{q-1}$

又是 F 的全部非零元素. 于是

$$x_1 \cdot \cdots \cdot x_{q-1} = (ax_1)\cdots(ax_{q-1}) = a^{q-1}x_1\cdots x_{q-1}.$$

由于 $x_1\cdots x_{q-1}\neq 0$. 从而 $a^{q-1}=1$，于是 $a^q=a$. 即 F 中每个非零元素均是多项式 $f(x)=x^q-x=x^{p^n}-x$ 的根，0 显然也是 $f(x)$的根，从而 F 恰好是由 $f(x)$的所有根组成的集合. 但是 p^n 次多项式 $f(x)$在域 Ω_p 中只有 p^n 个根. 这就表明 Ω_p 中只有唯一的一个 p^n 元域，即定理 1.4.2 中所述的那个域. 证毕.

今后我们把 Ω_p 中唯一的 $q=p^n$ 元有限域记为 $\boldsymbol{F}_q$.

在理论上，前三个定理的结论是很漂亮的. 但从实用的角度看来，则有很大的不足：我们不能明确写出 $\boldsymbol{F}_q$ 中 q 个元素的具体形式，更不能具体作四则运算，为了更为具体地构作出 q 元有限域，需要进一步研究 $\boldsymbol{F}_q$ 的结构.

对每个域 F，今后以 F^* 表示 F 的非零元素全体. 我们在第 1.1 节中说过，$\boldsymbol{F}_p^*$ 中存在本原元素 g，使得 $\boldsymbol{F}_p^*$ 中每个元素均可写成 g^i 的形式. 现在我们对任意有限域 $\boldsymbol{F}_q$ 来证明这件事.

$\boldsymbol{F}_q^*$ 中每个元素 a 均满足 $a^{q-1}=1$(见定理 1.4.3 的证明). 与前一样，我们把使 $a^n=1$ 成立的最小正整数 n 叫作 a 的阶. 可象定理 1.1.10 一样地证明：

(1) 若 a 为 n 阶元素，$N\in \mathbf{Z}$. 则 $a^N=1 \Longleftrightarrow n\mid N$. 特别地，$\boldsymbol{F}_q^*$ 中每个元素的阶均是 $q-1$ 的因子.

(2) 若 a 为 n 阶元素，$m\in \mathbf{Z}$，则 a^m 是 $\frac{n}{(n,m)}$ 阶元素. 特别地，a^m 为 n 阶元素的充要条件是$(n,m)=1$. 从而在 n 个不同元素$a,a^2,\cdots,a^{n-1},a^n=1$ 当中，n 阶元素的个数为 $\varphi(n)$，这里 $\varphi(n)$ 为欧拉函数，即等于 $1,2,\cdots,n$ 当中与 n 互素的个数.

1.4.4 引理 设 n 为正整数. 则

$$\sum_{d|n}\varphi(d)=n.$$

其中求和表示 d 取不超过 n 的所有正因子.

(例:对于 $n=6$, $\sum_{d|6}\varphi(d)=\varphi(1)+\varphi(2)+\varphi(3)+\varphi(6)=1+1+2+2=6$.)

证明 让我们用复数域中的一个模型来证明此引理. 令 $c=e^{\frac{2\pi i}{n}}$. 则 c 是 n 阶元素,即 n 是满足 $c^n=1$ 的最小正整数. 从而 $S=\{1,c,\cdots,c^{n-1}\}$ 是 n 元集合,而对于 $1\leqslant m\leqslant n$, c^m 的阶为 $\frac{n}{(n,m)}$. 从而阶只能是 n 的因子. 而对 n 的每个正因子 d,S 中阶为 d 的个数即是 $(n,m)=\frac{n}{d}$ 的 m 的个数. 如果 $(n,m)=\frac{n}{d}$, $1\leqslant m\leqslant n$,令 $m=\frac{n}{d}m'$,其中 m' 为正整数,$1\leqslant m'\leqslant d$. 则 $\frac{n}{d}=(n,m)=\frac{n}{d}(d,m')$. 于是 $(d,m')=1$. 这就表明 S 中阶为 d 的元素个数为满足 $(d,m')=1(1\leqslant m'\leqslant d)$ 的 m' 的个数,即等于 $\varphi(d)$. 现在把 S 中元素按阶分类. 对每个 $d|n$,d 阶元素共有 $\varphi(d)$ 个,而 S 中共有 n 个元素. 从而 $n=\sum_{d|n}\varphi(d)$.

1.4.5 定理 设 $q=p^n$,则 F_q^* 中必有 $q-1$ 阶元素,并且共有 $\varphi(q-1)$ 个 $q-1$ 阶元素. 对 $q-1$ 的每个正因子 d,F_q^* 中共有 $\varphi(d)$ 个 d 阶元素.

证明 根据上述,F_q^* 中元素的阶均为 $q-1$ 的因子. 对于 $q-1$ 的正因子 d,我们以 N_d 表示 F_q^* 中 d 阶元素的个数. F_q^* 中每个 d 阶元素均是 x^d-1 的根. 若 F_q^* 中存在 d 阶元素 a,则 x^d-1 的全部根为 $1,a,a^2,\cdots,a^{d-1}$. 而 F_q^* 中全部 d 阶元素都在它们之中. 但是我们知道其中恰有 $\varphi(d)$ 个 d 阶元素. 从而 N_d 或者

为零，或者为 $\varphi(d)$. 特别地，$N_d \leqslant \varphi(d)$. 我们把 F_q^* 中 $q-1$ 个元素按阶分类，对每个 $d|q-1$，d 阶元素有 N_d 个，于是

$$q-1=\sum_{d|q-1} N_d \leqslant \sum_{d|q-1} \varphi(d)=q-1$$

（最后等式是由引理 1.4.4）. 于是上式中间也为等号，并且对每个 $d|q-1$，$N_d=\varphi(d)$，即 F_q^* 中恰有 $\varphi(d)$ 个 d 阶元素. 特别地，恰有 $\varphi(q-1)$ 个 $q-1$ 阶元素. 由于 $\varphi(q-1)\geqslant 1$.（对每个正整数 n，由于 1 与 n 互素，由欧拉函数定义知 $\varphi(n)\geqslant 1$.）从而 F_q^* 中必存在 $q-1$ 阶元素.

1.4.6 定义 F_q^* 中 $q-1$ 阶元素叫作 q 元域 F_q 的**本原元素**.

由定理 1.4.5 知，F_q 共有 $\varphi(q-1)$ 个本原元素，对于 F_q 中任一本原元素 g，F_q 的 q 个元素分别为 $0,1,g^1,g^2,\cdots,g^{q-2}$（$g^{q-1}=1$）. 所以有限域的乘法结构是很简单的：

$$0\cdot g^i=0, \quad g^i\cdot g^j=g^{i+j}.$$

但是 F_q 的加法结构还不清楚：$g^i+g^j=?$. 所以还要继续深入讨论. 下面是构作有限域的另一种方法.

1.4.7 定理 设 $q=p^n$，$f(x)$ 为 $F_p[x]$ 中的 n 次不可约首 1 多项式. 若 α 是 $f(x)$（在 Ω_p 中）的一个根，则集合

$$S=\{c_0\alpha^{n-1}+c_1\alpha^{n-2}+\cdots+c_{n-1}\,|\,c_0,\cdots,c_{n-1}\in F_p\}$$

是一个 q 元域.

证明 首先证明集合 S 共有 q 个元素. 由于 $(c_0,c_1,\cdots,c_n)$ 一共有 $p^n=q$ 种取法，我们只需证明：对于 $(c_0,c_1,\cdots,c_n)$ 的不同取法，元素 α 彼此不同. 如果

$$c_0\alpha^{n-1}+c_1\alpha^{n-2}+\cdots+c_{n-1}$$

$$=c_0'\alpha^{n-1}+c_1'\alpha^{n-2}+\cdots+c_{n-1}'$$

其中 $c_i,c_i'\in \boldsymbol{F}_p$. 令 $d_i=c_i-c_i'\ (0\leqslant i\leqslant n-1)$，则

$$d_{\alpha}^{n-1}+d_1\alpha^{n-2}+\cdots+d_{n-1}=0.\quad d_i\in\boldsymbol{F}_p.$$

从而 α 是 $\boldsymbol{F}_p[x]$ 中多项式 $g(x)=d_0x^{n-1}+\cdots+d_{n-1}$ 的根. 如果 $g(x)\neq 0$，由于 $\deg g\leqslant n-1<n=\deg f$，而 f 不可约，因此 $g(x)$ 与 $f(x)$ 互素. 所以有 $A(x),B(x)\in\boldsymbol{F}_p[x]$，使得 $A(x)f(x)+B(x)g(x)=1$. 将 $x=\alpha$ 代入，便给出矛盾：$1=A(\alpha)f(\alpha)+B(\alpha)g(\alpha)=A(\alpha)\cdot 0+B(\alpha)\cdot 0=0$. 这表明 $g(x)=0$，即 $c_i-c_i'=d_i=0$，于是 $c_i=c_i'\ (0\leqslant i\leqslant n-1)$. 这就证明了 S 中共有 q 个元素.

再证 S 是域. 集合 S 为域 Ω_p 的子集，易知 S 中可进行加法运算，因为若 $a,b\in S$，则

$$a=c_0\alpha^{n-1}+c_1\alpha^{n-2}+\cdots+c_{n-1},$$
$$b=c_0'\alpha^{n-1}+c_1'\alpha^{n-2}+\cdots+c_{n-1}'.$$

其中 $c_i,c_i'\in\boldsymbol{F}_p$ 于是

$$a+b=(c_0+c_1')\alpha^{n-1}+\cdots+(c_{n-1}+c_{n-1}')\in S.$$

至于乘法，令 $A(x)=c_0x^{n-1}+c_1x^{n-2}+\cdots+c_{n-1}$，$B(x)=c_0'x^{n-1}+c_1'x^{n-2}+\cdots+c_{n-1}'$，则在 $\boldsymbol{F}_p[x]$ 中有除法算式

$$A(x)B(x)=q(x)f(x)+r(x).$$

其中 $q(x),r(x)\in\boldsymbol{F}_p[x]$，$r(x)=0$ 或者 $\deg r(x)<\deg f(x)=n$. 因此 $r(x)$ 可以写成 $r(x)=d_0x^{n-1}+d_1x^{n-2}+\cdots+d_{n-1}$，$d_i\in\boldsymbol{F}_p$. 于是

$$ab=A(\alpha)B(\alpha)=q(\alpha)\cdot 0+r(\alpha)\quad(\text{由于 } f(\alpha)=0)$$
$$=r(\alpha)=d_0\alpha^{n-1}+d_1\alpha^{n-2}+\cdots+d_{n-1}\in S.$$

所以 S 中也可进行乘法运算，进而，若 $a\in S$，易知 $-a\in S$. 最后若 $a\neq 0$，则 $A(x)\neq 0$. 但是 $\deg A(x)\leqslant n-1<\deg f(x)$，而 $f(x)$ 不可约，所以 $A(x)$ 与 $f(x)$ 互素. 因此有 $\lambda(x),\mu(x)\in$

$F_p[x]$,使得

$$f(x)\lambda(x)+A(x)\mu(x)=1.$$

将 $x=\alpha$ 代入,由于 $f(\alpha)=0, a=A(\alpha)$,从而得到 $a\cdot\mu(\alpha)=1$. 由集合 S 的定义可知 $\alpha\in S, F_p\subseteq S$. 而 S 中可以作加法和乘法,从而 $\mu(\alpha)\in S$. 这就表明当 $0\neq a\in S$ 时,a 在 S 中有逆元素 $\mu(\alpha)$. 综合上述,我们便知集合 S 是 q 元域.

采用定理1.4.7的办法构造出的有限域,容易进行四则运算. 但是我们仍旧留下一个问题. 用这种办法构作 p^n 元域需要 $F_p[x]$中一个 n 次不可约首1多项式. 那末,对于每个素数 p 和正整数 n,$F_p[x]$中是否一定存在 n 次不可约首1多项式?

1.4.8 引理 对每个素数 p 和正整数 n,$F_p[x]$中必存在 n 次不可约首1多项式.

证明 我们已经知道 $q=p^n$ 元有限域 F_q 是存在的(定理1.4.2),我们也知道 F_q 中存在本原元素 g(定理1.4.5),并且 g 是 $x^{q-1}-1$的根. 将 $x^{q-1}-1$作因式分解:

$$x^{q-1}-1=f_1(x)\cdots f_s(x),$$

其中 $f_i(x)(1\leqslant i\leqslant s)$为 $F_p[x]$中不可约首1多项式. 则 g 必为某个 $f_i(x)$的根. 不妨设 $f_1(g)=0$.

设 $\deg f_1(x)=m$. 由定理1.4.7知

$$S=\{c_0g^{m-1}+c_1g^{m-2}+\cdots+c_{m-1}\mid c_0,\cdots,c_{m-1}\in F_p\}$$

是 p^m 元域. 而 $F_q=\{0,1,g,\cdots,g^{q-2}\}$. 我们证明事实上两个域 S 和 F_q 相等. 由于 $g\in S$,从而每个 g^i 均属于域 S. 于是 $F_q\subseteq S$. 另一方面,由于 $g\in F_q, F_p\subseteq F_q$,又可知 S 中每个元素均属于 F_q,即 $S\subseteq F_q$. 于是 $S=F_q$,而 S 有 p^m 个元素,从而 $p^m=q=p^n$. 于是 $n=m$,即 $f_1(x)$为 $F_p[x]$中 n 次不可约首1多项式. 证毕.

注记 下节我们要计算 $F_p[x]$中 n 次不可约多项式的确切

个数.

以上我们对于有限域的存在性，唯一性和构作方法均给出了比较满意的答案，现在举两个例子.

例1 x^2+x+2为$F_3[x]$中的不可约多项式(若x^2+x+2可约，则它必有一次多项式因子，即它在F_3中有根. 但是$f(0)=f(2)=2\neq 0, f(1)=1\neq 0$. 这表明$x^2+x+2$在$F_3[x]$中不可约). 所以按定理1.4.7的方式可用$x^2+x+2$构作$F_9$. 设$\alpha$为$x^2+x+2$的一个根，则$\alpha^2+\alpha+2=0$. 即

$$\alpha^2 = 2\alpha + 1.$$

根据定理1.4.7. F_9的9个元素为

$$0,\ 1,\ 2,\ \alpha,\ \alpha+1,\ \alpha+2,\ 2\alpha,\ 2\alpha+1,\ 2\alpha+2.$$

并且反复利用$\alpha^2=2\alpha+1$，可以得出

$$\alpha^3=\alpha(2\alpha+1)=2\alpha^2+\alpha=2(2\alpha+1)+\alpha=2\alpha+2,$$

$$\alpha^4=\alpha(2\alpha+2)=2\alpha^2+2\alpha=2(2\alpha+1)+2\alpha=2(=-1),$$

$$\alpha^5=2\alpha,\quad \alpha^6=\alpha+2,\quad \alpha^7=\alpha+1,\quad \alpha^8=1.$$

这表明α是8阶元素，即是F_9的本原元素. 如果我们把元素$c_0\alpha+c_1(c_0,c_1\in F_3)$简写成$(c_0,c_1)$. 那末$F_9$中每个元素和它们的两种表达方式可列成下表：(其中$\alpha^2=2\alpha+1,\alpha^8=1$)

$$0=(0,0),\qquad \alpha^2=(2,1),\qquad \alpha^5=(2,0),$$

$$1=(0,1),\qquad \alpha^3=(2,2),\qquad \alpha^6=(1,2),$$

$$\alpha=(1,0),\qquad \alpha^4=(0,2)(=-1),\qquad \alpha^7=(1,1).$$

乘法可用左边的表达方式来作：

$$(2\alpha+1)(\alpha+2)=(2,1)\cdot(1,2)(\text{查表})$$

$$=\alpha^2\cdot\alpha^6=\alpha^8=1(=(0,1)).$$

加法则用右边的表达方式来作：

$$\alpha^3+\alpha^5=(2,2)+(2,0)=(1,2)=\alpha^6.$$

例2 $x^4+x^3+x^2+x+1$是$F_2[x]$中不可约多项式(因为

$F_2[x]$中次数$\leqslant 2$的不可约多项式$x, x+1, x^2+x+1$均不是它的因子). 设α是此多项式的一个根. 则$\alpha^4=\alpha^3+\alpha^2+\alpha+1$. 并且$F_{16}$中元素可表成

$$c_0\alpha^3+c_1\alpha^2+c_2\alpha+c_3=(c_0, c_1, c_2, c_3) \quad (c_i \in F_2).$$

易知$\alpha^5=1$. 从而α不是F_{16}中本原元素. 我们最好找到一个本原元素(因为这时F_{16}^*中每个元素均可表成它的方幂). 记$\gamma=1+\alpha$, 则必然$\gamma^{15}=1$. 因此γ的阶只能是1, 3, 5或15. 但是经计算知

$$\gamma \neq 1,$$

$$\gamma^3=\gamma \cdot \gamma^2=(1+\alpha)(1+\alpha)^2=(1+\alpha)(1+\alpha^2)$$
$$=1+\alpha+\alpha^2+\alpha^3 \neq 1,$$

$$\gamma^5=(1+\alpha)(1+\alpha)^4=(1+\alpha)(1+\alpha^4)=1+\alpha+\alpha^4+\alpha^5$$
$$=1+\alpha+\alpha^4+(\alpha+\alpha^2+\alpha^3+\alpha^4)=1+\alpha^2+\alpha^3 \neq 1.$$

从而γ是本原元素. 由于α是$f(x)=x^4+x^3+x^2+x+1$的根, 所以$\gamma=1+\alpha$是$f(x+1)=(x+1)^4+(x+1)^3+(x+1)^2+(x+1)+1=x^4+x^3+1$的根. 于是

$$\gamma^4=\gamma^3+1.$$

F_{16}^*中每个元素即可表成$\gamma^i (0 \leqslant i \leqslant 14)$, 又可表成$c_0\gamma^3+c_1\gamma^2+c_2\gamma+c_3=(c_0, c_1, c_2, c_3)$ $(c_i \in F_2)$. 于是F_{16}中全部元素和它们的两种表示法为 $(\gamma^4=\gamma^3+1, \gamma^{15}=1)$.

$$0=(0,0,0,0), \qquad \gamma^7=(0,1,1,1),$$
$$1=(0,0,0,1), \qquad \gamma^8=(1,1,1,0),$$
$$\gamma=(0,0,1,0), \qquad \gamma^9=(0,1,0,1),$$
$$\gamma^2=(0,1,0,0), \qquad \gamma^{10}=(1,0,1,0),$$
$$\gamma^3=(1,0,0,0), \qquad \gamma^{11}=(1,1,0,1),$$
$$\gamma^4=(1,0,0,1), \qquad \gamma^{12}=(0,0,1,1),$$
$$\gamma^5=(1,0,1,1), \qquad \gamma^{13}=(0,1,1,0),$$
$$\gamma^6=(1,1,1,1), \qquad \gamma^{14}=(1,1,0,0).$$

最后我们谈谈有限域之间的互相包含关系. 如果 p 和 p' 是不同的素数，$q=p^n$，$q'=(p')^m$，则有限域 F_q 和 F_q' 不会一个包含一个. 因为它们的特征 p 和 p' 不同. 现在我们固定一个素数 p. 如果 $m>n$，则 F_{p^m} 中元素个数比 F_{p^n} 中元素个数多. 自然以为 F_{p^n} 一定是 F_{p^m} 的子域. 但这是不对的.

1.4.9 定理 设 p 为素数，n 和 m 为正整数. 则：

$$F_{p^n}\subseteq F_{p^m}\Longleftrightarrow n\mid m.$$

证明 F_{p^n} 中元素是 $x^{p^n}-x$ 的根，F_{p^m} 中元素是 $x^{p^m}-x$ 的根. 当 $n|m$ 时，

$$x^{p^m}-x=(x^{p^n}-x)(x^{p^{m-n}}+x^{p^{m-2n}}+\cdots+x^p+1),$$

所以 F_{p^n} 中元素一定是 F_{p^m} 中元素. 即 $F_{p^n}\subseteq F_{p^m}$. 反之，若 $F_{p^n}\subseteq F_{p^m}$，则 $m\geqslant n$. 取 F_{p^n} 中一个本原元素 g，则 g 的阶为 p^n-1. 但是 $g\in F_{p^m}$，从而 $g^{p^m-1}=1$. 于是 $p^n-1\mid p^m-1$. 考虑除法算式 $m=\lambda n+r$，$\lambda,r\in\mathbf{Z}$，$0\leqslant r<n$. 则

$$\frac{p^m-1}{p^n-1}=\frac{p^{\lambda n+r}-p^r}{p^n-1}+\frac{p^r-1}{p^n-1}=p^r\left(\frac{p^{\lambda n}-1}{p^n-1}\right)+\frac{p^r-1}{p^n-1}.$$

由于 $m\geqslant n$，从而 $\lambda\geqslant 1$. 于是 $\dfrac{p^{\lambda n}-1}{p^n-1}=p^{(\lambda-1)n}+p^{(\lambda-2)n}+\cdots+p^n+1\in\mathbf{Z}$. 因此 $p^n-1\mid p^r-1$. 再由 $0\leqslant r<n$ 可知必然 $r=0$，即 $m=\lambda n$. 从而 $n|m$. 证毕.

1.4.10 习 题

1. 设 $q=p^n$，求证 F_q 中每个元素 a 在 F_q 中均可开 p 次方，即必存在 $b\in F_q$，使得 $a=b^p$.
2. 设 k 为正整数. 求证：F_q 中每个元素在 F_q 中均可开 k 次方的充要条件

是$(q-1,k)=1$.

3. 设 n 为奇数,$a,b\in F_{2^n}$. 求证 $a^2+ab+b^2=0\Longrightarrow a=b=0$.

4. 设$2\nmid q$. 求证:F_q^* 中元素 a 在 F_q^* 中可开平方的充要条件是 $a^{\frac{q-1}{2}}=1$. 由此证明 F_q^* 中共有$\frac{q-1}{2}$个这样的元素. 如果$2|q$,则 F_q 中每个元素均可在 F_q 中开平方.

5. 设 $a\in F_q$,n 为正整数,求证在 $F_q[x]$中,$x^q-x+a\mid x^{q^n}-x+na$.

6. 设 $a,b,\in F_q^*$. 求证对每个 $c\in F_q$,方程

$$ax^2+by^2=c$$

在 F_q 中均有解.

7. 求证 $F_{p^n}\cap F_{p^m}=F_{p^d}$,其中 $d=(n,m)$.

8. 求证当 $n\geqslant3$时,$x^{2^n}+x+1$是 $F_2[x]$中可约多项式.

9. 设 n 和 t 为正整数,$m=nt$. 求证 F_{p^m}中每个本原元素必是 $F_{p^n}[x]$中某个 t 次不可约多项式的根. 由此证明:对每个 $q=p^n$ 和每个正整数 t,$F_q[x]$中均存在 t 次不可约首1多项式.

10. 设 k 为正整数. 求证

$$\sum_{a\in F_q}a^k=\begin{cases}0, & \text{如果}(q-1)\nmid k\\ -1, & \text{否则}\end{cases}$$

11. 设 $c\in F_q$,$q=p^n$. 求证

   (1) 方程 $x^p-x+c=0$在 F_q 中或者无根,或者有 p 个根.

   (2) F_q 中恰好有 p^{n-1}个元素 a,使得方程 $x^p-x+a=0$在 F_q 中有解.

   (3) 若 x^p-x+c 在 F_q 中无解,则它在 $F_q[x]$中不可约.

12. 设 $c\in F_q^*$. 求证对每个正整数 k,

   (1) 方程 $x^k=c$ 在 F_q^* 中或者无解,或者恰好有$(k,q-1)$个解.

   (2) F_q^* 中恰好有$\frac{q-1}{(k,q-1)}$个元素 a,使得方程 $x^k=a$ 在 F_q^* 中有解.

13. 设$1\neq a\in F_q$,$b\in F_q$. 求证 x^q-ax-b 在 $F_q[x]$中可约.

14. 设 $b\in F_p^*$. 求证:x^p-x-b 在 $F_{p^n}[x]$中不可约$\Longleftrightarrow p\nmid n$.

15. 设 r 为素数,$a\in F_q$. 求证 x^r-a 或者在 $F_q[x]$中不可约,或者在 F_q 中有根.

16. 设$2\nmid q$. 则多项式$\frac{1}{2}(1+x^{\frac{q+1}{2}}+(1-x)^{\frac{q+1}{2}})$为$F_q[x]$中某个多项式的平方.

§1.5 有限域上的多项式

在第1.3节我们论述了任意域上多项式的一般性质. 本节讲有限域上多项式的一些特殊性质.

1.5.1 定理 设$f(x)$是$F_q[x]$中n次不可约多项式，$\deg f\geqslant 1$. α为$f(x)$的一个根. 则

(1)包含F_q和α的最小域为F_{q^n}.

(2)$f(x)$的全部根为$\alpha,\alpha^q,\alpha^{q^2},\cdots,\alpha^{q^{n-1}}$. 并且这$n$个根彼此不同.

(3)对于$F_q[x]$中每个多项式$g(x)$，α为$g(x)$的根当且仅当$f(x)|g(x)$.

证明 (1) 我们可以象定理1.4.7的证明中那样，推出集合

$$S=\{c_0\alpha^{n-1}+c_1\alpha^{n-2}+\cdots+c_{n-1}|c_0,\cdots,c_{n-1}\in F_q\}$$

是q^n元域(定理1.4.7是对$q=p$的情形证明的. 对于q为素数幂的一般情形其证明完全一样). 若域F包含F_q和α，由S定义知F也包含S. 这就表明$S=F_{q^n}$是包含F_q和α的最小域.

(2) 设$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n, a_i\in F_q$. 则$a_0\alpha^n+a_1\alpha^{n-1}+\cdots+a_{n-1}\alpha+a_n=f(\alpha)=0$. 由$a_i\in F_q$可知$a_i^q=a_i$. 从而

$$\begin{aligned}0&=(a_0\alpha^n+a_1\alpha^{n-1}+\cdots+a_{n-1}\alpha+a_n)^q\\&=(a_0\alpha^n)^q+(a_1\alpha^{n-1})^q+\cdots+(a_{n-1}\alpha)^q+a_n^q\\&=a_0(\alpha^q)^n+a_1(\alpha^q)^{n-1}+\cdots+a_{n-1}\alpha^q+a_n\end{aligned}$$

$$=f(\alpha^q).$$

这就表明 α^q 为 $f(x)$的根. 从而 $\alpha^{q^2}=(\alpha^q)^q,\alpha^{q^3},\cdots,\alpha^{q^{n-1}}$ 均是 $f(x)$ 的根. 再证 $\alpha,\alpha^q,\alpha^{q^2},\cdots,\alpha^{q^{n-1}}$ 彼此不同(于是它们就是 $f(x)$的全部根). 如果 $\alpha^{q^i}=\alpha^{q^j}$, 其中$0\leqslant i<j\leqslant n-1$. 令 $m=j-i$, 则$1\leqslant m\leqslant n-1$. 由(1)知 $\alpha\in F_{q^n}$, 从而 $\alpha^{q^n}=\alpha$. 于是

$\alpha=\alpha^{q^n}=(\alpha^{q^i})^{q^{n-i}}=(\alpha^{q^j})^{q^{n-i}}=\alpha^{q^{n+j-i}}=\alpha^{q^{j-i}}=\alpha^{q^m}$. 这表明 $\alpha\in F_{q^m}$. 从而 F_q 和 α 均包含在 F_{q^m}之中. 但是 $m<n$, 这就与(1)中结论相矛盾. 从而 $\alpha,\alpha^q,\cdots,\alpha^{q^{n-1}}$彼此不同.

(3)若 $f(x)\mid g(x)$, 易知 α 为 $g(x)$的根. 反之若 α 为 $g(x)$的根, 可以象(1)中那样证明 $\alpha,\alpha^q,\cdots,\alpha^{q^{n-1}}$均为 $g(x)$的根. 现在我们将 $f(x)$和 $g(x)$在 $F_{q^n}[x]$中分解. 由于 $\alpha,\alpha^q,\cdots,\alpha^{q^{n-1}}$为 $f(x)$ 的全部根, 并且没有重根, 可知在 $F_{q^n}[x]$中 $f(x)=a(x-\alpha)\cdot(x-\alpha^q)\cdots(x-\alpha^{q^{n-1}})$其中 $a\in F_q^*$ 为 $f(x)$的首项系数. 又因 $\alpha,\alpha^q,\cdots,\alpha^{q^{n-1}}$也均为 $g(x)$的根. 从而 $g(x)=(x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^{n-1}})\cdot h(x)$. 于是在 $F_{q^n}[x]$中 $f(x)\mid g(x)$, 所以在 $F_q[x]$中也有 $f(x)\mid g(x)$.

注记 通常以 $F_q(\alpha)$表示定理1.5.1的(1)中所述的包含 F_q 和 α 的最小域. 它也叫作将元素 α 添加到 F_q 之中而得到的扩域.

如果 α 属于 F_q 的某个有限扩域, 我们一定能求得 $F_q[x]$中一个不可约首1多项式 $f(x)$以 α 为根. 这是因为: 若 α 属于 F_q 的有限扩域 F_{q^n}, 则 α 是 $x^{q^n}-x$ 的根. 将 $x^{q^n}-x$ 在 $F_q[x]$中分解成

$$x^{q^n}-x=f_1(x)\cdots f_l(x),$$

其中 $f_1,\cdots,f_l$ 均是 $F_q[x]$中不可约首1多项式, 那末 $0=\alpha^{q^n}-\alpha=f_1(\alpha)\cdots f_l(\alpha)$. 从而必有某个 $f_i(\alpha)=0$. 即 α 是 $F_q[x]$中首1不

可约多项式 $f_i(x)$的根.

又由定理1.5.1的(3)知道，$F_q[x]$中每个以 α 为根的多项式均是 $f_i(x)$的倍式. 所以我们通常把 $f_i(x)$叫作 α 在 $F_q[x]$中的**极小多项式**.

问题是：给了 α 之后，如何去求 α 在 $F_q[x]$中的极小多项式?

1.5.2 定理 设 α 是 F_q 的某个有限扩域中的元素. 若 n 是使 $\alpha^{q^n}=\alpha$ 成立的最小正整数. 则

$$f(x)=(x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^{n-1}})$$

就是 α 在 $F_q[x]$中的极小多项式.

证明 我们先证 $f(x)$是 $F_q[x]$中的多项式. 设

$$\begin{aligned} f(x)&=(x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^{n-2}})(x-\alpha^{q^{n-1}}) \\ &=x^n+c_1x^{n-1}+c_2x^{n-2}+\cdots+c_n. \end{aligned} \tag{1}$$

我们要证 $c_1,\cdots,c_n\in F_q$. 为此将(1)式乘 q 次方，便得到(注意 $\alpha^{q^n}=\alpha$)：

$$\begin{aligned} &(x^q-\alpha^q)(x^q-\alpha^{q^2})\cdots(x^q-\alpha^{q^{n-1}})(x^q-\alpha) \\ &=(x^q)^n+c_1^q(x^q)^{n-1}+c_2^q(x^q)^{n-2}+\cdots+c_n^q. \end{aligned} \tag{2}$$

此式两边均为 x^q 的多项式. 将(1)式中的 x 改成 x^q，然后与(2)式比较，即知 $c_1^q=c_1,\cdots,c_n^q=c_n$. 因此 $c_1,\cdots,c_n\in F_q$. 即 $f(x)\in F_q[x]$.

$F_q[x]$中每个多项式 $g(x)$若以 α 为根，则 $\alpha^q,\cdots,\alpha^{q^{n-1}}$均是 $g(x)$的根. 由此即知 $f(x)\mid g(x)$. 从而 $f(x)$是 α 在 $F_q[x]$中的极小多项式. 从而 $f(x)$也必为 $F_q[x]$中的不可约多项式. 证毕.

例 让我们回到上一节的例2. 在这个例子中我们构作了域 $F_{16}=F_2(\gamma)$，其中 γ 为 F_{16}中本原元素，$\gamma^{15}=1,\gamma^4=\gamma^3+1$. 那里还

给出 F_{16}中所有元素的两种表达方式.

由于 γ^5是3阶元素,从而它是 F_4的本原元素. 于是 F_4中4个元素为0, $\gamma^5=(1,0,1,1)$, $\gamma^{10}=(1,0,1,0)=\gamma^5+1$,和 $\gamma^{15}=1$. 即 $F_4=\{0,\gamma^5,\gamma^5+1,1\}$.

现在求 γ^2在 $F_4[x]$中的极小多项式 $f(x)$. 由于$(\gamma^2)^4=\gamma^8$, $(\gamma^2)^{4^2}=(\gamma^8)^4=\gamma^{32}=\gamma^2$. 根据定理1.5.2, $f(x)$以 γ^2和 γ^8为根. 因此

$$f(x)=(x-\gamma^2)(x-\gamma^8)=x^2-(\gamma^2+\gamma^8)x+\gamma^{10}.$$

由于 $\gamma^2+\gamma^8=(0,1,0,0)+(1,1,1,0)=(1,0,1,0)=\gamma^{10}(=\gamma^5+1)$,从而 γ^2在 $F_4[x]$中的极小多项式为 $x^2+\gamma^{10}x+\gamma^{10}$.

让我们再求 γ^5在 $F_2[x]$中的极小多项式 $g(x)$. 由于$(\gamma^5)^2=\gamma^{10}$, $(\gamma^{10})^2=\gamma^{20}=\gamma^5$. 从而 $g(x)$的根为 γ^5和 γ^{10}. 于是 $g(x)=(x+\gamma^5)(x+\gamma^{10})=x^2+(\gamma^5+\gamma^5+1)x+\gamma^{15}=x^2+x+1$. 由此也可看出 $\gamma^5\in F_4$.

我们在引理1.4.8中证明了对每个素数 p 和正整数 n, $F_p[x]$中必然存在 n 次不可约首1多项式. 将 p 改成 $q=p^k$,那里的证明仍旧适用. 即对每个 $n\geqslant 1$, $F_q[x]$中均有 n 次不可约首1多项式. 现在我们计算 $F_q[x]$中 n 次不可约首1多项式的确切个数. 在计算中我们要用到初等数论中一个函数(叫作 Möbius 函数),它定义为

$$\mu(n)=\begin{cases}(-1)^l, & \text{如果 } n \text{ 是 } l \text{ 个不同素数之积.}\\ 0, & \text{否则.}\end{cases}$$

例如: $\mu(1)=1$, $\mu(2)=\mu(3)=\mu(5)=\mu(7)=-1$, $\mu(4)=\mu(8)=\mu(9)=\mu(12)=0$, $\mu(6)=\mu(10)=1$.

我们还要用到初等数论的一个反演公式:

1.5.3 引理 设 $f(n)$和 $g(n)$均是数论函数(即自变量取正整数). 如果对每个正整数 n 均有

$$f(n)=\sum_{d\mid n}g(d),$$

则对每个正整数 n 均有

$$g(d)=\sum_{d\mid n}\mu(d)f\left(\frac{n}{d}\right)\left(=\sum_{d\mid n}\mu\left(\frac{n}{d}\right)f(d)\right).$$

这里求和均是 d 过 n 的所有正因子.

证明 参见任何一本初等数论的书.

例 我们曾经在引理1.4.4中证明了

$$n=\sum_{d\mid n}\varphi(d).$$

取 $f(n)=n, g(n)=\varphi(n)$, 用反演公式便给出欧拉函数的表达式

$$\varphi(n)=\sum_{d\mid n}\mu(d)\frac{n}{d}=n\sum_{d\mid n}\frac{\mu(d)}{d}. \qquad (*)$$

设 $n=p_1^{a_1}p_2^{a_2}\cdots p_s^{a_s}$ 是 n 的标准分解式. 由 $\mu(n)$ 的定义知, 当 n 的因子 d 被某个素数 p_i 的平方除尽时, $\mu(d)=0$, 这对于(*)式后边求和没有贡献. 而当 d 为 s 个不同素数 $p_1,\cdots,p_s$ 当中任意 l 个之积时, $\mu(d)=(-1)^l$. 于是(*)式变成

$$\begin{aligned}\varphi(n)&=n\left(1-\sum_{i=1}^{s}\frac{1}{p_i}+\sum_{1\leqslant i<j\leqslant s}\frac{1}{p_ip_j}-\cdots+(-1)^s\frac{1}{p_1p_2\cdots p_s}\right)\\&=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_s}\right)\\&=n\cdot\prod_{p\mid n}\left(1-\frac{1}{p}\right).\end{aligned}$$

其中上式右边乘积表示 p 过 n 的所有素因子.

1.5.4 定理 (1) 设 $f(x)$ 是 $F_q[x]$ 中首1不可约多项式,

则：$f(x)\mid x^{q^n}-x \Longleftrightarrow \deg f\mid n$.

(2) $x^{q^n}-x$ 等于 $\boldsymbol{F}_q[x]$ 中所有次数除尽 n 的不可约首1多项式之积.

(3) $\boldsymbol{F}_q[x]$ 中 n 次不可约首1多项式的个数为 $\frac{1}{n}\sum_{d\mid n}\mu(d)q^{\frac{n}{d}}$.

证明 (1) 令 $\deg f=d$. 如果 $f(x)\mid x^{q^n}-x$. 设 α 是 $f(x)$ 的根，则 $\boldsymbol{F}_q(\alpha)=\boldsymbol{F}_{q^d}$（定理1.5.1的(1)）. 由于 $f(x)\mid x^{q^n}-x$，从而 α 也是 $x^{q^n}-x$ 的根. 即 $\alpha\in\boldsymbol{F}_{q^n}$. 由于 $\boldsymbol{F}_{q^d}$ 是包含 $\boldsymbol{F}_q$ 和 α 的最小域，因此 $\boldsymbol{F}_{q^d}$ 为 $\boldsymbol{F}_{q^n}$ 的子域. 于是 $d\mid n$（定理1.4.9）. 反之设 $d\mid n$. 则 $\boldsymbol{F}_{q^d}=\boldsymbol{F}_q(\alpha)\subseteq\boldsymbol{F}_{q^n}$. 于是 $\alpha\in\boldsymbol{F}_{q^n}$. 从而 α 是 $x^{q^n}-x$ 的根. 由于 $f(x)$ 不可约，并且 $f(\alpha)=0$，所以 $f(x)$ 是 α 在 $\boldsymbol{F}_q[x]$ 中的极小多项式. 于是 $f(x)\mid x^{q^n}-x$（定理1.5.1的(3)）.

(2) 由(1)直接推出.

(3) 结论(2)可表示成

$$x^{q^n}-x=\prod_{d\mid n}\prod_{\substack{\deg f=d\\ \text{首1,不可约}}}f(x), \qquad (*)$$

其中第二个乘积表示 f 过 $\boldsymbol{F}_q[x]$ 中所有 d 次不可约首1多项式. 如果以 $N(n)$ 表示 $\boldsymbol{F}_q[x]$ 中 n 次不可约首1多项式的个数，则考虑(*)式两边多项式的次数，便得到

$$q^n=\sum_{d\mid n}dN(d).$$

在反演公式（引理1.5.3）中取 $f(n)=q^n$，$g(n)=nN(n)$，便由上式得到

$$nN(n)=\sum_{d\mid n}\mu(d)q^{\frac{n}{d}},$$

从而 $\boldsymbol{F}_q[x]$ 中 n 次不可约首1多项式个数为

$$N(n)=\frac{1}{n}\sum_{d\mid n}\mu(d)q^{\frac{n}{d}}.$$

设 $f(x)$ 为 $F_q[x]$ 中 n 次不可约首1多项式，α 是 $f(x)$ 的一个根. 则 $F_q(\alpha)=F_{q^n}$. 但是 α 不一定为 F_{q^n} 的本原元素（见第1.4节的例2）. 不难证明：若 $f(x)$ 的一个根 α 是 F_{q^n} 的本原元素，则 $f(x)$ 的所有根 $\alpha,\alpha^q,\alpha^{q^2},\cdots,\alpha^{q^{n-1}}$ 均是 F_{q^n} 的本原元素.

1.5.5定义 设 $f(x)$ 为 $F_q[x]$ 中 n 次不可约首1多项式. 如果 $f(x)$ 的根 α 是 F_{q^n} 的本原元素，我们称 $f(x)$ 为 $F_q[x]$ 中本原多项式.

1.5.6 定理 $F_q[x]$ 中 n 次本原多项式共有 $\frac{1}{n}\varphi(q^n-1)$ 个.

证明 F_{q^n} 中共有 $\varphi(q^n-1)$ 个本原元素（定理1.4.5）. 每个本原元素都是 $F_q[x]$ 中某个 n 次本原多项式 $f(x)$ 的根，而这样 $f(x)$ 的 n 个根均是 F_{q^n} 中（不同的）本原元素. 所以 $F_q[x]$ 中 n 次本原多项式的个数为 $\frac{1}{n}\varphi(q^n-1)$.

例 $F_2[x]$ 中4次本原多项式的个数为

$$\frac{1}{4}\varphi(2^4-1)=\frac{1}{4}\varphi(15)=\frac{1}{4}\cdot 15\cdot\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)=2.$$

而4次不可约（首1）多项式的个数为

$$\frac{1}{4}\sum_{d\mid 4}\mu(d)2^{\frac{4}{d}}=\frac{1}{4}(\mu(1)2^4+\mu(2)2^2)$$

$$=\frac{1}{4}(16-4)=3.$$

由于 $F_2[x]$ 中不可约多项式 $f(x)$ 的常数项必为1（否则 $x\mid f(x)$），并且 $f(x)$ 共有奇数个项（否则 $f(1)=0$，即 $(x+1)\mid$

$f(x)$). 因此只需考虑

$$x^4+x^3+1, x^4+x^2+1, x^4+x+1, x^4+x^3+x^2+x+1,$$

由于 $x^4+x^2+1=(x^2+x+1)^2$,从而其余三个多项式都是不可约的. 又由于 $x^4+x^3+x^2+x+1$的根 α 是5阶的,即不是 F_{16}中的本原元素,从而 x^4+x^3+1和 x^4+x+1是 $F_2[x]$中的本原多项式.

最后我们谈谈有限域上多项式的另一个特性:多项式的周期.

1.5.7 定义 设 $f(x)$是 $F_q[x]$中多项式,$f(0)\neq 0$(这等价于 $x\nmid f(x)$). 如果存在正整数 n,使得 $f(x)\mid x^n-1$,则满足这一性质的最小正整数 n 叫作 $f(x)$的**周期**,表示成 $P(f)$.

注记 若 $f(0)=0$,则 $x\mid f(x)$. 由于对每个 n,$x\nmid x^n-1$,从而 $f(x)\nmid x^n-1$. 这说明当 $f(0)=0$时,$f(x)$没有周期概念. 下面定理表明,当 $f(0)\neq 0$(即 $f(x)$的常数项不为0)时,$f(x)$必有周期. 并且还给出周期的求法.

1.5.8 定理 设 $f(x)\in F_q[x]$, $\deg f\geqslant 1$, $f(0)\neq 0$.

(1) 若 $f(x)$的周期为 $P(f)$,则 $f(x)\mid x^m-1 \Longleftrightarrow P(f)\mid m$.

(2) 若 $f(x)$为 $F_q[x]$中不可约多项式. 则 $P(f)$等于 $f(x)$的每个根的阶,特别地:$f(x)$为 $F_q[x]$中 n 次本原多项式$\Longleftrightarrow P(f)=q^n-1$.

(3) 设 $f(x)=g(x)^b$,其中 b 为正整数,$g(x)$为 $F_q[x]$中不可约多项式. $q=p^m$. $P(g)=e$. 令 t 是满足 $p^t\geqslant b$ 的最小整数,则 $P(f)=ep^t$.

(4)设 $f(x)=f_1(x)f_2(x)\cdots f_s(x)$,其中 $f_1,\cdots,f_s$ 是 $F_q[x]$

中彼此互素的多项式，则

$$P(f)=[P(f_1),\cdots,P(f_s)]\quad（最小公倍数）.$$

证明 (1) 若 $P(f)|m$，显然 $f(x)|(x^{P(f)}-1)|x^m-1$. 反之，若 $f(x)|x^m-1$. 考虑除法算式

$$m=q\cdot P(f)+r,\quad 0\leqslant r<P(f).$$

则 $x^m-1=(x^m-x^r)+(x^r-1)=x^r(x^{qP(f)}-1)+(x^r-1)$. 由于 $f(x)|x^m-1$，$f(x)|(x^{q\cdot P(f)}-1)$，从而 $f(x)|x^r-1$. 再由 $P(f)$的定义即知 $r=0$. 于是 $m=q\cdot P(f)$，即 $P(f)|m$.

(2) 设 α 是 $F_q[x]$中不可约多项式 $f(x)$的任意一个根. 则：

$$f(x)|x^n-1\Longleftrightarrow(x-\alpha)|x^n-1\quad（定理1.5.1的(3)）$$
$$\Longleftrightarrow\alpha^n=1.$$

由于 $f(0)\neq0$，故 $\alpha\neq0$. 从而存在正整数 n 使得 $\alpha^n=1$. 因此 $f(x)|x^n-1$. 于是 $f(x)$存在周期 $P(f)$，并且由定义知 $P(f)$为满足$f(x)|x^n-1$的最小正整数. 由上式可知 $P(f)$为满足 $\alpha^n=1$ 的最小正整数，即 $P(f)$等于 α 的阶，其中 α 是 $f(x)$任意一个根.

(3) 由 $g(x)|x^e-1$可知 $g(x)^b|g(x)^{p^t}|(x^e-1)^{p^t}=x^{ep^t}-1$. 由(1)知 $P(g^b)|ep^t$. 另一方面，设 $d=\deg g(x)$. 则 $g(x)|x^{q^d-1}-1$ (由于 $g(x)$不可约并且 $g(0)\neq0$). 于是 $e|q^d-1$. 从而$(e,p)=1$. 进而由 $g(x)|g(x)^b|x^{p(g^b)}-1$可知 $e|p(g^b)|ep^t$. 再由$(e,p)=1$即知 $P(g^b)=ep^l$，其中 $l\leqslant t$. 从而 $g(x)^b|x^{ep^l}-1=(x^e-1)^{p^l}$. 由于不可约多项式 $g(x)$没有重根，而 x^e-1也没有重根(因为$(e,p)=1$，从而$(x^e-1,(x^e-1)')=(x^e-1,ex^{e-1})=(x^e-1,x^{e-1})=1$). 再由 $g(x)^b|(x^e-1)^{p^l}$即知 $b\leqslant p^l$. 再由 t 的定义可知 $l\geqslant t$. 于是 $l=t$. 即 $P(f)=P(g^b)=ep^t$.

(4) 由于

$$f(x)|x^n-1\Longleftrightarrow f_i(x)|x^n-1(1\leqslant i\leqslant s)$$

$$\Longleftrightarrow P(f_i)\mid n(1\leqslant i\leqslant s)$$
$$\Longleftrightarrow [P(f_1),\cdots,P(f_s)]\mid n.\text{（习题1.1.11,(1)）}$$
从而 $P(f)=[P(f_1),\cdots,P(f_s)]$，因为此等式两边分别为满足 $f(x)\mid x^n-1$ 和 $[P(f_1),\cdots,P(f_s)]\mid n$ 的最小正整数 n.

定理1.5.8完全给出了计算 $\boldsymbol{F}_q[x]$ 中多项式 $f(x)(f(0)\neq 0)$ 的周期的方法.

例 $f(x)=(x^2+x+1)^3(x^4+x+1)\in\boldsymbol{F}_2[x]$. 易知 x^2+x+1 的周期为3. 由于 x^4+x+1 是 $\boldsymbol{F}_2[x]$ 中本原多项式，从而它的周期为 $2^4-1=15$（上述定理的(2)）. 根据上述定理的(3)知 $(x^2+x+1)^3$ 的周期为 $3\cdot 2^2=12$.. 再根据上述定理的(4)即知 $f(x)$ 的周期为 $[12,15]=60$.

1.5.9 习 题

1. 设 $f(x)$ 为 $\boldsymbol{F}_q[x]$ 中 n 次不可约多项式，k 为正整数. $d=(k,n)$. 求证：$f(x)$ 在 $\boldsymbol{F}_{q^k}[x]$ 中分解成 d 个 $\frac{n}{d}$ 次不可约多项式之积.
2. 写出 $\boldsymbol{F}_3[x]$ 中所有三次首1不可约多项式和三次本原多项式.
3. 求证：$\boldsymbol{F}_q[x]$ 中每个 m 次首1不可约多项式均是本原多项式 $\Longleftrightarrow q=2$ 并且 2^m-1 为素数.
4. 设 $n\geqslant 2$. 求证 $\boldsymbol{F}_q[x]$ 中所有 n 次不可约首1多项式之乘积等于
$$\prod_{d\mid n}(x^{q^d-1}-1)^{\mu(n/d)}.$$
5. 求 $\boldsymbol{F}_2[x]$ 中多项式 $(x^2+x+1)^5(x^3+x+1)$ 的周期.
6. (Ⅰ) 求证 $\sum\limits_{d\mid n}\frac{\mu(d)}{d}=\frac{\varphi(n)}{n}$.

   (Ⅱ) 求证 $x^{q^n}-x$ 在 $\boldsymbol{F}_q[x]$ 中首1不可约多项式因子的个数为
   $$\frac{1}{n}\sum_{d\mid n}\varphi(d)q^{n/d}.$$

7. 利用定理1.5.4证明 $F_q[x]$ 中 n 次首1不可约多项式的个数 $N(n)$ 有如下的估计：

$$\frac{1}{n}(q^n-q)\geqslant N(n)\geqslant\frac{1}{n}q^n-\frac{q}{n(q-1)}(q^{n/2}-1).$$

并且：$N(n)=\frac{1}{n}(q^n-q)\Longleftrightarrow n$ 为素数.

8. 利用(7)题中对 $N(n)$ 的下界估计证明 $N(n)\geqslant 1$. 即对每个 q 和 n，$F_q[x]$ 中均有 n 次不可约多项式.

9. 证明 x^5-x+1 为 $F_3[x]$ 中本原多项式.

第二章　有限域的应用

前面讲述了有限域的构作方式和它们的代数结构，以及有限域上多项式的特殊性质. 所谓代数结构，就是对某种集合赋以一个或多个运算，并且这些运算满足某些特定的法则(或叫定律). 数学中研究的各种结构五花八门(除了代数结构之外，还有几何结构，拓扑结构，解析结构，序结构等). 有些是(或者一开始是)从兴趣出发，但就整体而言，或者从根本上说，这些数学结构的研究是各种实际领域和数学自身逻辑发展的需要(兴趣也是人类向自己的智慧和能力挑战的一种需求意识). 人们对于各种需要或目标的不同理解，给出各种数学结构的不同价值标准. 一般来说，如果对某种数学结构所加条件愈多，要求也愈苛刻. 这种结构也就愈少，但也就更为具体. 就拿我们在第1.2节定义的域这种代数结构来说，它有四则运算并且满足通常的运算法则. 条件已经不少. 但是人们对域的研究远未终结，其中对两种特殊域的研究产生了数学的两大分支：研究有理数域和它的(有限次)扩域的，叫作代数数论；研究有理函数域 $F(x)$ 或者 $F(x_1, x_2, \cdots, x_n)$ 和它们的(有限次)扩域的，叫作代数几何，可是，只要对域再加上一个非常简单的“有限”条件. 第1.4节充分表明，这

种有限域一下子就有非常具体的结构.至少在理论上它是非常清楚的.这表明域的有限性这一条件虽然简单,但是却非常强.

有限域的简洁而美妙的特性被应用到各种实际领域中,作为构造各种组合结构的有效工具.所谓组合结构,即是用某个集合中的元素构作成具有某种对称(或平衡)性质的各种构图.这种构图常常体现出图形上的数学美.有些组合结构起源于数学游戏.但是当发现它们有实际应用,或者认识到它们在数学和其他科学上的深刻含义之后,便又促使人们对它作更认真更深入地研究.

综合上述,用具有良好代数性能的有限代数结构——有限域为工具,构作各种美妙的有限组合结构,应当是顺理成章的事.顺着这个道理我们写成的这一章,就是要举一些用有限域构作组合构图的实例.

§2.1 有限射影平面

我们在中学里学习过平面几何,研究了平面上各种图形的几何性质.就拿直线来说,两条不同直线的位置关系有两种:或者只交于一点,或者平行.我们也知道,过直线 l 外任意一点恰好有一条直线与 l 平行.公元前3世纪,希腊数学家欧几里德(Euclid)写《几何原本》时,把这件事作为公理,以后许多年里,人们一直认为这条平行公理可以从其他公理推出,并且为了“证明”平行公理,有人甚至耗费了毕生精力,后来才发现平行公理与欧氏几何的所有其他公理是独立的.他们构作了一些非欧几何的“模型”,在这些模型中,除了平行公理之外,欧氏几何所有其他公理均成立,但是平行公理不对.这些非欧几何分成两大

类：一类是“球面几何”，在这种几何中，任意两条不同直线均相交. 这种几何用于天文和航海上. 另一种是“双曲几何”，在这种几何模型中，过直线 l 外一点可引许多条直线与 l 平行，这种几何后来在物理世界中得到反映.

我们现在要讲的射影几何完全是一种组合结构. 使用几何中的名词只不过是想使事情的叙述更为形象.

2.1.1 定义 集合 π 叫作是一个**射影平面**，是指我们给出集合 π 的一些特定的子集，每个子集叫作一条**直线**，而 π 中每个元素叫作一个**点**. 并且满足下列三个条件：

(P1) π 中任意两个不同点恰好在一条公共直线上.

(P2) π 中任意两条不同直线恰好交于一点.

(P3) π 中存在四个不同的点，使得其中任意三点均不同时在一条直线上.

设 π 是射影平面. 如果 π 为有限集合，则 π 叫作**有限射影平面**.

我们先举一个有限射影平面的例子：下面图形便是一个有限射影平面. 整个平面 π 由七个点组成：

$$\pi=\{A,B,C,A',B',C',O\}.$$

图1中除了六条通常直线之外，由虚线画出的圆也是一条直线. 从而共有下面七条直线：

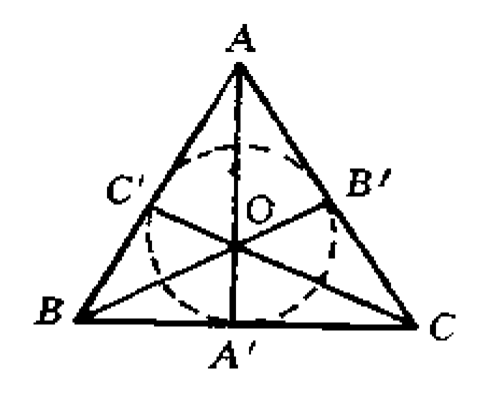


图1

$\{AC'B\},\{BA'C\},\{CB'A\},\{AOA'\},\{BOB'\},\{COC'\},$
$\{A'B'C'\}$

每条直线上有三个点. 从图形中可看出它满足射影平面的三条

公理(例如对公理($P3$),我们可以取四个点 A,B,C,O).

有限射影平面的研究起源于上个世纪中期.最基本问题是:我们可以构作出哪些有限射影平面?这个问题至今未能完全解决.目前已经构作出来的所有有限射影平面全是利用有限域.在讲具体构作方法之前,我们想再谈一点射影平面的性质.

射影平面的所有性质均应从三条公理(P1),(P2)和(P3)推出.注意(P1)和(P2)是彼此对偶的:即只要把"点"改成"直线",把"直线"改成"点",把"点在直线上"改成"直线过点",那末(P1)就变成(P2),而(P2)就变成(P1).类似地,公理(P3)的对偶命题应当叙述成:

(P4)π 中存在四条不同直线,它们当中任意三条直线均不交于同一点.

事实上,(P4)可以从前三条公理推出,从而它也是任意射影平面的特性.现在我们来证明(P4):设 P_1,P_2,P_3,P_4是(P3)中所给出的四个点.则它们任意三点均不共线.由公理(P1)知道过 P_1和 P_2恰好有一条直线,我们记作$\overline{P_1P_2}$.同样有直线$\overline{P_2P_3}$,$\overline{P_3P_4}$,$\overline{P_4P_1}$.现在我们证明这四条直线满足(P4)的要求.先证这是四条不同的直线.例如,若$\overline{P_1P_2}=\overline{P_2P_3}$,则点 P_1,P_2,P_3在同一直线上,与假设矛盾.其余情形类似.再证任三条直线均不交于一点.比如考虑直线$\overline{P_1P_2}$,$\overline{P_2P_3}$,它们交于点 P_2.根据($P2$)知它们只有这一个交点,从而可表示成$\overline{P_1P_2}\cap\overline{P_2P_3}=P_2$,类似知$\overline{P_2P_3}\cap\overline{P_3P_4}=P_3\neq P_2$,从而$\overline{P_1P_2}$,$\overline{P_2P_3}$和$\overline{P_3P_4}$不能有公共交点.同样可证其他情形.于是我们证明了(P4).由于(P3)和(P4)也是相互对偶的.而射影平面上的所有性质均由(P1)到(P4)推出来.可知若一个命题在射影平面中正确,那末它的对偶命题在射影平面中也正确.射影平面上的这个**对偶原则**,体现了射影平面的一种内在美.

2.1.2 定理 设 π 是有限射影平面，则

(1) 任意两条直线上的点数相等.

(2) 过点 P 的直线数等于过另一点 P' 的直线数.

(3) 直线 l 上的点数等于过点 P 的直线数.

(4) 设(1)到(3)中那个公共数字为 $n+1$，则 π 中共有 n^2+n+1 个点和 n^2+n+1 条直线.

证明 (1) 设 l 和 l' 是 π 中两条不同直线. 我们先证 π 中必有点 O 既不在 l 上也不在 l' 上. 因为若不然，则 π 中所有的点均或在 l 上或在 l' 上. 但是由(P3)我们有四个点，其中任意三点均不共线. 所以必然其中两点 A 和 B 在 l 上，而另两点 C 和 D 在 l' 上. 然后易知直线 $\overline{AC}$ 和 $\overline{BD}$ 的交点 O 既不在 l 上又不在 l' 上(请读者自证).

现在设点 O 既不在 l 上又不在 l' 上. 对于 l 上每个点 P，由于 $O\notin l'$ (这表示点 O 不在直线 l' 上)，可知 $\overline{OP}\neq l'$. 于是 $\overline{OP}$ 和 l' 交于一点 P'. 由此给出从直线 l 到直线 l' 的一个映射 σ，即 $\sigma(P)=P'$，其中 P' 由上述方式作出(这个映射通常叫作以点 O 为中心的投射，如图所示). 现在证明 $\sigma: l\to l'$ 是一一对应. 如果又有 $Q\in l$，$\sigma(Q)=P'$，并且 $Q\neq P$. 则两条不同直线 l 和 $\overline{OP'}$ 就有两个交点 P 和 Q，这与(P1)矛盾. 因此 σ 为单射，即 l 中不同的点通过 σ 映成 l' 中不同的点. 另一方面，

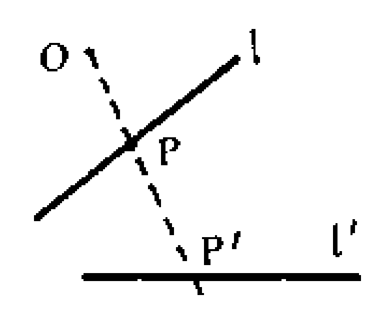


图2

对于 l' 上每个点 Q'，必然 $\overline{OQ'}\neq l$ (因为点 O 不在 l 上). 从而 $\overline{OQ'}$ 和 l 有交点 Q，易知 $\sigma(Q)=Q'$ (为什么?). 从而 σ 为满射，于是 $\sigma: l\to l'$ 为一一对应. 这就表明直线 l 和 l' 有相同的点数.

(2) 是(1)的对偶命题. 所以由(1)正确自然得出(2)的正确性.

(3) 由于过每点的直线数相同，每条直线上的点数也相同，我们不妨取点 P 不在直线 l 上(由公理($P3$)知存在不在一条直线上的三点 P,A,B. 于是点 P 便不在直线 $\overline{AB}=l$ 上). 于是，过点 P 的每条直线 l_i 均不为 l，从而 l_i 与 l 交于一点 Q_i. 易知 $l_i \to Q_i$ 是过 P 的诸直线与 l 上诸点之间的一一对应. 于是，过点 P 的直线数等于 l 上的点数.

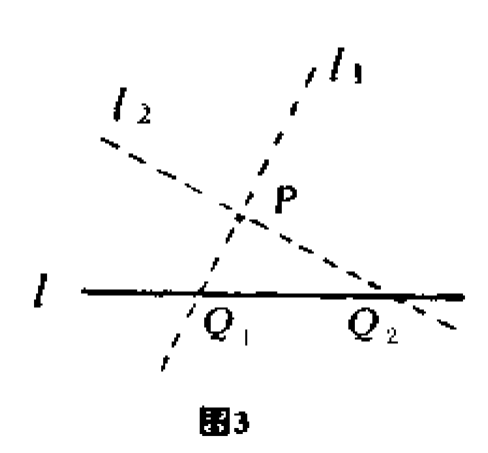


图3

(4) 过点 O 共有 $n+1$ 条直线 $l_1,\cdots,l_{n+1}$. π 中除了点 O 之外，每个点 P 均在唯一的一条直线 l_i 上(因为 $P\neq O$，由公理(P1)，过 P 和 O 有唯一直线，它们必是某个 l_i). 每条直线 l_i 上除了点 O 之外还有 n 个点. 并且不同的直线 l_i 和 l_j 只有一个公共交点(公理(P2)). 所以 π 中点的总数为 $1+n(n+1)=n^2+n+1$. 再由对偶原则，π 中直线总数也是 n^2+n+1.

2.1.3 定义 每条直线上均恰有 $n+1$ 个点的有限射影平面叫作 **n阶射影平面**。

前面的例子是一个2阶射影平面. 一个自然的问题是：对于每个正整数 n，是否均存在 n 阶射影平面?

每个学过平面几何的人都有体会：作几何题需要很高的智能和技巧. 法国数学家笛卡儿的重要贡献是在平面上引进坐标. 平面上的点用它的坐标 (x,y) 来表示，其中 x 和 y 为实数. 而实

数集合是一个域，即有四则运算. 平面上的几何图形用方程表示，几何性质的证明归结为在实数域上解方程组. 这就是解析几何，即用代数方法研究欧氏几何. 现在我们也可以用域 F 来建立射影几何. 我们主要谈射影平面. 并且域 F 可以是任意的，不必是实数域.

设 F 为域，S 为 F 上不全为零的三元组全体构成的集合，即

$$S=\{(a_0,a_1,a_2)\mid a_0,a_1,a_2\in F,(a_0,a_1,a_2)\neq(0,0,0)\}.$$

我们再把 S 中许多元素看成是等同的. 确切地说，如果存在域中非零元素 $\alpha\in F$，使得

$$a_0=\alpha a_0',\quad a_1=\alpha a_1',\quad a_2=\alpha a_2',$$

（这也写作 $(a_0,a_1,a_2)=\alpha(a_0',a_1',a_2')$），便称 S 中元素 (a_0,a_1,a_2) 和 (a_0',a_1',a_2') 是**等价**的. 我们用 $[a_0,a_1,a_2]$ 表示所有与 S 中元素 (a_0,a_1,a_2) 等价的元素全体，即

$$[a_0,a_1,a_2]=\left\{(a_0',a_1',a_2')\,\middle|\,\begin{array}{l}\text{存在 }\alpha\in F^*\text{，使得}\\(a_0',a_1',a_2')=\alpha(a_0,a_1,a_2)\end{array}\right\}$$

最后，我们把所有 $[a_0,a_1,a_2]$ 组成的集合记成 $\pi(F)$.

例1 取 $F=\mathbf{F}_3$，则非零的三数组 (a_0,a_1,a_2)（其中 $a_0,a_1,a_2\in\mathbf{F}_3$）共有 $3^3-1=26$ 个. 所以 S 中共有26个元素. 由于 (a_0,a_1,a_2) 和 $(2a_0,2a_1,2a_2)$ 等价. 所以每个 $[a_0,a_1,a_2]$ 包含 S 中两个元素. 因此 $\pi(\mathbf{F}_3)$ 中共有13个元素. 由于 $[a_0,a_1,a_2]=2[a_0,a_1,a_2]$，因此当 $a_0\neq0$ 时，我们总可取 $a_0=1$. 所以这时共给出 $\pi(\mathbf{F}_3)$ 中下列9个元素：

$$[1,a_1,a_2],\quad 0\leqslant a_1,a_2\leqslant 2.$$

而当 $a_0=0$ 时还有4个元素：$[0,1,0]$，$[0,1,1]$，$[0,1,2]$，$[0,0,1]$

仍设 F 为任意的域. 我们把 $\pi(F)$ 中的元素叫作是**点**. 设

x_0, x_1, x_2为 F 中不全为零的元素. 考虑(变量为 a_0, a_1, a_2的)方程

$$a_0x_0 + a_1x_1 + a_2x_2 = 0. \tag{1}$$

如果 S 中元素(a_0, a_1, a_2)满足方程(1),那末对每个 $\alpha \in F^*$, $\alpha(a_0, a_1, a_2) = (\alpha a_0, \alpha a_1, \alpha a_2)$也满足方程(1). 从而我们可以说 $\pi(F)$中的点$[a_0, a_1, a_2]$满足方程(1). 我们把满足(1)式的 $\pi(F)$中所有点$[a_0, a_1, a_2]$组成的集合叫作 $\pi(F)$的一条**直线**,并且把这个直线表示成$\langle x_0, x_1, x_2\rangle$,即

$$\langle x_0, x_1, x_2\rangle = \{[a_0, a_1, a_2] \mid a_0x_0 + a_1x_1 + a_2x_2 = 0\}.$$

2.1.4 引理 设 $x_0, x_1, x_2, y_0, y_1, y_2 \in F$, x_0, x_1, x_2不全为零, y_0, y_1, y_2也不全为零. 则

$$\langle x_0, x_1, x_2\rangle = \langle y_0, y_1, y_2\rangle \Longleftrightarrow \text{存在 } \alpha \in F^*, \text{使得}$$
$$\alpha x_i = y_i \quad (i = 0, 1, 2).$$

证明 $\Longleftarrow$: 假设 $\alpha x_i = y_i (i=0,1,2)$,其中 $\alpha \in F^*$. 那末:

点$[a_0, a_1, a_2]$在直线$\langle x_1, x_2, x_3\rangle$上

$\Longleftrightarrow a_0x_0 + a_1x_1 + a_2x_2 = 0$

$\Longleftrightarrow \alpha(a_0x_0 + a_1x_1 + a_2x_2) = 0$ (由于 $\alpha \neq 0$)

$\Longleftrightarrow a_0y_0 + a_1y_1 + a_2y_2 = 0$ (由于 $\alpha x_i = y_i$)

$\Longleftrightarrow$点$[a_0, a_1, a_2]$在直线$\langle y_0, y_1, y_2\rangle$上.

$\Longrightarrow$: 假设$\langle x_0, x_1, x_2\rangle$和$\langle y_0, y_1, y_2\rangle$为同一条直线. 由于 y_0, y_1, y_2不同时为零,我们不妨设 $y_0 \neq 0$. 由于点$[1, 0, 0]$不在直线$\langle y_0, y_1, y_2\rangle$上$(1 \cdot y_0 + 0 \cdot y_1, + 0 \cdot y_2 = y_0 \neq 0)$,从而点$[1, 0, 0]$也不在直线$\langle x_0, x_1, x_2\rangle$上(因为$\langle x_0, x_1, x_2\rangle = \langle y_0, y_1, y_2\rangle$). 于是$1 \cdot x_0 + 0 \cdot x_1 + 0 \cdot x_2 \neq 0$,即 $x_0 \neq 0$. 记 $\alpha x_0 = y_0$,于是 $\alpha \in F^*$. 因为 $x_0 \neq 0$,从而$[x_1, -x_0, 0]$是 $\pi(F)$中的点,并且易知此点在直线$\langle x_0, x_1, x_2\rangle$上,从而也在直线$\langle y_0, y_1, y_2\rangle$上. 于是 $x_1y_0 - x_0y_1 + 0 \cdot y_2 = 0$,即 $x_0y_1 = x_1y_0 = \alpha x_0x_1$. 由 $x_0 \neq 0$即知 $y_1 = \alpha x_1$. 同样可

证 $y_2=\alpha x_2$. 于是 $y_i=\alpha x_i(i=0,1,2)$.

例2 我们在例1中给出集合 $\pi(F_3)$ 中全部13个点. 从引理2.1.4可知 $\pi(F_3)$ 也恰好有13条直线. 直线 $\langle 1,1,2\rangle$ 上的点 $[a_0, a_1, a_2]$ 应当满足条件

$$a_0 + a_1 + 2a_2 = 0.$$

由此可算出,直线 $\langle 1,1,2\rangle$ 上共有四个点:$[1,0,1]$,$[1,1,2]$,$[1,2,0]$ 和 $[0,1,1]$. 类似地,过点 $[1,1,2]$ 的直线 $\langle x_0,x_1,x_2\rangle$ 应当满足条件

$$x_0 + x_1 + 2x_2 = 0,$$

从而过点 $[1,1,2]$ 也恰好有四条直线:$\langle 1,0,1\rangle$,$\langle 1,1,2\rangle$,$\langle 1,2,0\rangle$ 和 $\langle 0,1,1\rangle$.

从这个例子以及点 $[a_0,a_1,a_2]$ 在直线 $\langle x_0,x_1,x_2\rangle$ 上的方程 $a_0x_0+a_1x_1+a_2x_2=0$ 对称形式,可看出 $\pi(F)$ 中点和直线的对偶性质. 现在我们证明:

2.1.5 定理 对任意域 F,$\pi(F)$ 对于上面规定的点和直线是一个射影平面.

证明 我们只需验证定义2.1.1中的三条公理(P1),(P2)和(P3).

公理(P1) 设 $P=[a_0,a_1,a_2]$ 和 $Q=[b_0,b_1,b_2]$ 是 $\pi(F)$ 中两个不同的点. 每个通过此二点的直线 $\langle x_0,x_1,x_2\rangle$ 均是方程组

$$\begin{cases} a_0x_0 + a_1x_1 + a_2x_2 = 0, \\ b_0x_0 + b_1x_1 + b_2x_2 = 0 \end{cases}$$

的解. 由于 a_0,a_1,a_2 不全为零,不妨设 $a_0\neq 0$,从而可设 $a_0=1$. 于是

$$x_0 = - a_1x_1 - a_2x_2. \tag{1}$$

将此式代入方程组的第二个方程，得到

$$(b_1 - a_1b_0)x_1 + (b_2 - a_2b_0)x_2 = 0.$$

令 $c_1=b_1-a_1b_0, c_2=b_2-a_2b_0$，方程变成

$$c_1x_1 + c_2x_2 = 0. \tag{2}$$

如果 $c_1=c_2=0$，则 $b_1=a_1b_0, b_2=a_2b_0$. 于是 $P=[1,a_1,a_2]=b_0[1,a_1,a_2]=Q$，这与 P 和 Q 是两个不同的点相矛盾. 从而 c_1 和 c_2 不全为零. 这时，易知方程(2)在域 F 中的所有解可表成

$$x_1 = c_2t, \ x_2 = -c_1t, \quad (t \in F).$$

再代入(1)式，知 $x_0=(c_1a_2-c_2a_1)t$. 由于 x_0,x_1,x_2 不全为零，从而 $t\neq 0$. 因此过 P 和 Q 两点只有唯一的一条直线

$$\begin{aligned}\langle x_0,x_1,x_2\rangle &= \langle (c_1a_2-c_2a_1)t, c_2t, -c_1t\rangle \\ &= \langle c_1a_2-c_2a_1, c_2, -c_1\rangle.\end{aligned}$$

从(1)和对偶原则可得到(2)，或用类似于(1)的方式直接证(2).

(3)可直接验证[1,0,0]，[0,1,0]，[0,0,1]和[1,1,1]四点中任意三点均不共线. 例如考虑点[1,0,0]，[0,1,0]和[1,1,1]三点. 若三点均在直线 $\langle x_0,x_1,x_2\rangle$ 上，则 x_0,x_1,x_2 均不为零. 但是这三点在此直线上又得到方程 $x_0=0, x_1=0, x_0+x_1+x_2=0$. 从而也有 $x_2=-x_0-x_1=0$ 这不可能，其余情形类似.

注记 对于熟悉线性代数的读者，证明本定理是件非常容易的事情.

定理2.1.5表明，对于每个域 F 我们总可得到一个射影平面 $\pi(F)$. 如果要构作有限射影平面，自然想到利用有限域 F_q. 在 F_q 上共有 q^3-1 个非零的 (a_0,a_1,a_2). 其中每 $q-1$ 个彼此等价(即彼此相差 F_q^* 中一个元素作因子)，从而 $\pi(F_q)$ 中共有 $(q^3-1)/(q-1)=q^2+q+1$ 个点. 由定理2.1.2的(4)可知 $\pi(F_q)$ 是 q 阶射影平面. 这就证明了

2.1.6 定理 对每个素数幂 q,均存在 q 阶射影平面.

由于 $\pi(F_q)$是 q 阶射影平面,所以由定理2.1.2可知,每条直线上恰有 $q+1$个点,而每个点都恰好在 $q+1$条直线上.取 $q=2$, $\pi(F_2)$中共有七个点:

$$A=[1,0,0],\quad B=[0,1,0],\quad C=[0,0,1],$$
$$A'=[0,1,1],\ B'=[1,0,1],\ C'=[1,1,0],$$
$$O=[1,1,1].$$

而七条直线分别为:

$$\langle 0,0,1\rangle=\overline{AC'B},\ \langle 1,0,0\rangle=\overline{BA'C},\ \langle 0,1,0\rangle=\overline{CB'A},$$
$$\langle 0,1,1\rangle=\overline{AOA'},\ \langle 1,0,1\rangle=\overline{BOB'},\ \langle 1,1,0\rangle=\overline{COC'},$$
$$\langle 1,1,1\rangle=\overline{A'B'C'},$$

画出图形来,可知这就是本节一开始所举的例子.

如果我们用组合学的语言,则2阶射影平面给出了七元集合 $\pi(F_2)=\{A,B,C,A',B',C',O\}$的七个子集$\{A,C',B\}\{B,A',C\}\{C,B',A\}\{A,O,A'\}\{B,O,B'\}\{C,O,C'\}\{A',B',C'\}$.
其中任意两个不同子集均恰有一个公共元素,任意两个不同的元素均恰好同时在一个子集之中.每个元素均恰好有3个子集包含它,每个子集均有3个元素.这是一种非常有对称性(或平衡性)的组合构图.我们在第2.3节中还要提到它.

由定理2.1.6可知,阶数为2,3,4,5,7,8,9,11,…的有限射影平面均是存在的.自然要问:6阶和10阶的射影平面是否存在?利用穷举法已经证明了6阶射影平面是不存在的.而10阶射影平面是否存在,是一个长期未解决的著名数学难题.其主要困难是当 n 不为素数幂时,研究 n 阶射影平面缺少象有限域那样好的工具.1988年底,林永康教授利用电脑证明了10阶有限射影平面不存在,详见附录.

利用相当深刻的代数数论知识,Bruck 和 Ryser 证明了:若 $n\equiv 1$或者$2 \pmod 4$,n 没有平方因子,并且 n 有素因子 $p\equiv 3 \pmod 4$,则不存在 n 阶有限射影平面. 由此即知不存在6阶,14阶,21阶,22阶……的射影平面. 除了定理2.1.6的肯定性结果和上述 Bruck—Ryser 的否定性结果之外,所有其他 n 阶($n=12,15,18,20,\cdots$)射影平面的存在性问题均未解决.

2.1.7 习 题

1. 构作3阶射影平面.
2. 求证:对任意域 F,射影平面 $\pi(F)$中两条不同直线$\langle x_0,x_1,x_2\rangle$和$\langle y_0,y_1,y_2\rangle$的交点为

$$\left[\begin{vmatrix} x_1 & x_2 \\ y_1 & y_2 \end{vmatrix}, \begin{vmatrix} x_2 & x_0 \\ y_2 & y_0 \end{vmatrix}, \begin{vmatrix} x_0 & x_1 \\ y_0 & y_1 \end{vmatrix}\right]$$

   其中$\begin{vmatrix} a & b \\ c & d \end{vmatrix}=ad-bc$(二阶行列式).
   写出此命题的对偶命题.
3. 求证射影平面 $\pi(F)$(F 为域)中三个不同的点$[a_0,a_1,a_2]$,$[b_0,b_1,b_2]$和$[c_0,c_1,c_2]$在一条直线上的充要条件是三阶行列式

$$\begin{vmatrix} a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 \\ c_0 & c_1 & c_2 \end{vmatrix}$$

   等于零. 写出它的对偶命题.

§2.2 正交拉丁方

设 S 是一个 n 元集合. 不妨设 $S=\{1,2,\cdots,n\}$. $n\geq 2$. S 上的一个 n阶方阵 A 是指 n^2个数按下列方式排成一个 n 行 n 列的方

块

$$A=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ & \cdots\cdots\cdots & & \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

其中每个 a_{ij} 都是 S 中的元素. 这个 n 阶方阵也简记为 $A=(a_{ij})_{n\times n}$，或 $A=(a_{ij})$. 其中元素 a_{ij} 位于第 i 行第 j 列的交叉处.

如果 A 的每一行和每一列的 n 个元素均恰好是 $1,2,\cdots,n$ 这 n 个数(排列次序可不同)，称 A 是一个 **n阶拉丁方**. 例如

$$A=(a_{ij})=\begin{vmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{vmatrix}, \quad B=(b_{ij})=\begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}$$

都是三阶拉丁方. 一般地，对于 $(1,2,\cdots,n)$ 的任意一个排列 $(a_1, a_2,\cdots,a_n)$，则

$$\begin{bmatrix} a_1 & a_2 & a_3 & \cdots & a_{n-1} & a_n \\ a_2 & a_3 & a_4 & \cdots & a_n & a_1 \\ a_3 & a_4 & a_5 & \cdots & a_1 & a_2 \\ & & \cdots\cdots\cdots\cdots & & & \\ a_n & a_1 & a_2 & \cdots & a_{n-2} & a_{n-1} \end{bmatrix}$$

是 n 阶拉丁方.

将上面所举两个三阶拉丁方 $A=(a_{ij})$ 和 $B=(b_{ij})$ 重叠在一起，即把 A 和 B 在同一位置 (i,j) 处的两个元素 a_{ij} 和 b_{ij} 合并成 (a_{ij},b_{ij})，便得到合并方阵

$$\begin{bmatrix} (1,1) & (2,2) & (3,3) \\ (2,3) & (3,1) & (1,2) \\ (3,2) & (1,3) & (2,1) \end{bmatrix}$$

我们发现对集合 $S=\{1,2,3\}$ 中任意两个数 a,b 在合并方阵中

恰好有一个(a,b). 于是合并方阵中的九个(a_{ij},b_{ij})恰好就是$(a,b)(1\leqslant a,b\leqslant 3)$全体. 这样的两个拉丁方叫作是正交的. 换句话说,两个 n 阶拉丁方 $A=(a_{ij})$和 $B=(b_{ij})$叫作是正交的,是指对任意两个 $a,b\in\{1,2,\cdots,n\}$,均存在方阵唯一的位置(i,j)(表示第 i 行第 j 列交叉处),使得$(a_{ij},b_{ij})=(a,b)$.

二阶拉丁方只有两个:

$$\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix},\quad \begin{pmatrix}2 & 1\\ 1 & 2\end{pmatrix}.$$

它们不是正交的,从而不存在二阶正交拉丁方.

关于正交拉丁方的一个基本问题是:对于哪些 n,必存在正交拉丁方?如果存在 n 阶正交拉丁方,那么最多可以有多少个 n 阶拉丁方 $A_1,\cdots,A_t$,使得它们是两两正交的?

正交拉丁方问题起源于欧拉于1782年提出的所谓"三十六军官问题":有来自六个团队并且具有六种军衔的三十六名军官,每个团队里每种军衔都各有一名军官. 能否将这三十六名军官排成六行六列的方阵,使得每行和每列的六名军官,既来自不同的团队,又具有不同的军衔?

不难看出,这个问题相当于构作一对六阶正交拉丁方(第一个拉丁方中的1,2,…,6表示六个军衔,第二个拉丁方中的元素1,2,…,6则表示六个团队). 1900年,Tarry 用穷举法证明了不存在一对六阶正交拉丁方,即"三十六军官问题"是无解的. 欧拉根据二阶和六阶正交拉丁方均不存在这个事实,作出了大胆的猜想:对于每个正整数 $n\equiv 2 \pmod 4$,均不存在一对 n 阶正交拉丁方. 然而欧拉犯了一个大错误. 1959年,印度统计学家 Bose 等人彻底否定了欧拉这个猜想. 他们证明了,对于每个 $n\equiv 2 \pmod 4$, $n\geqslant 10$,均存在一对 n 阶正交拉丁方!后来,我国组合设计专家朱烈教授于1982年对此给出更为简洁和巧妙的证明(Zhu

Lie, A short disproof of Euler's conjecture concerning orthogonal Latin squares, Ars. Comb. 14 (1982)).

下面是一对10阶正交拉丁方：

$$
\begin{bmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\
7 & 8 & 1 & 2 & 3 & 5 & 6 & 9 & 10 & 4 \\
6 & 7 & 9 & 8 & 1 & 2 & 5 & 10 & 4 & 3 \\
5 & 6 & 7 & 10 & 9 & 8 & 1 & 4 & 3 & 2 \\
8 & 5 & 6 & 7 & 4 & 10 & 9 & 3 & 2 & 1 \\
10 & 9 & 5 & 6 & 7 & 3 & 4 & 2 & 1 & 8 \\
3 & 4 & 10 & 5 & 6 & 7 & 2 & 1 & 8 & 9 \\
9 & 10 & 4 & 3 & 2 & 1 & 8 & 7 & 6 & 5 \\
4 & 3 & 2 & 1 & 8 & 9 & 10 & 6 & 5 & 7 \\
2 & 1 & 8 & 9 & 10 & 4 & 3 & 5 & 7 & 6
\end{bmatrix}
$$

$$
\begin{bmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\
10 & 5 & 2 & 3 & 4 & 8 & 9 & 6 & 7 & 1 \\
7 & 1 & 8 & 2 & 3 & 4 & 6 & 9 & 10 & 5 \\
9 & 10 & 5 & 6 & 2 & 3 & 4 & 7 & 1 & 8 \\
4 & 7 & 1 & 8 & 9 & 2 & 3 & 10 & 5 & 6 \\
3 & 4 & 10 & 5 & 6 & 7 & 2 & 1 & 8 & 9 \\
2 & 3 & 4 & 1 & 8 & 9 & 10 & 5 & 6 & 7 \\
5 & 8 & 6 & 9 & 7 & 10 & 1 & 2 & 3 & 4 \\
8 & 6 & 9 & 7 & 10 & 1 & 5 & 3 & 4 & 2 \\
6 & 9 & 7 & 10 & 1 & 5 & 8 & 4 & 2 & 3
\end{bmatrix}
$$

现在我们给出两两正交 n 阶拉丁方个数的上界

2.2.1 定理 设 $A_1, \cdots, A_t$ 是两两正交的 n 阶拉丁方，则

$$t \leqslant n-1.$$

证明 设 A_1 的第一行为 $(c_1,\cdots,c_n)$，这是 $(1,2,\cdots,n)$ 的一种排列. 如果把 A_1 中所有数字 c_1 均改成1，c_2 均改成2，$\cdots$，c_n 均改成 n，所得仍为一个拉丁方，并且此时第一行为 $(1,\cdots,n)$. 我们今后把第一行为 $(1,2,\cdots,n)$ 的拉丁方叫作标准的. 采用同样办法，我们也把 $A_2,\cdots,A_t$ 都变成标准的拉丁方. 并且不难看出，这 t 个标准的拉丁方仍然是两两正交的. 所以我们不妨一开始就假定 $A_1,A_2,\cdots,A_t$ 是标准的两两正交的 n 阶拉丁方. 从而它们有形式

$$A_i=\begin{bmatrix} 1 & 2 & \cdots & n \\ d_i & * & \cdots & * \\ * & * & \cdots & * \\ & \cdots\cdots\cdots\cdots & & \end{bmatrix}$$

设拉丁方 A_i 在第2行第1列处为 d_i，则 $2\leqslant d_i\leqslant n$. 我们证明 $d_1,\cdots,d_t$ 彼此不同. 因若 $d_i=d_j=k,i\neq j,2\leqslant k\leqslant n$，则 A_i 和 A_j 重叠之后，在第2行第1列处和第1行第 k 列处都是 (k,k). 这和 A_i 与 A_j 正交相矛盾. 由于 $d_1,d_2,\cdots,d_t$ 是 $\{2,3,\cdots,n\}$ 中 t 个不同元素，从而 $t\leqslant n-1$. 证毕.

由定理2.2.1可知，两两正交的 n 阶拉丁方组最多有 $n-1$ 个拉丁方. 我们将 $n-1$ 个两两正交的 n 阶拉丁方叫作 n 阶**完备正交拉丁方组**. 现在我们用有限域来构作这样的完备正交拉丁方组.

2.2.2 定理 设 $q=p^m$（p 为素数，$m\geqslant1$）. 则当 $q\geqslant3$ 时，存在 q 阶完备正交拉丁方组.

证明 我们不用 $\{1,2,\cdots,q\}$ 这 q 个元素而改用有限域 $\boldsymbol{F}_q$ 中的 q 个元素，并且把它们记为

$$\boldsymbol{F}_q = \{a_0 = 0, a_1 = 1, a_2, \cdots, a_{q-1}\}.$$

考虑 $q-1$个 q 阶方阵 $A_1, A_2, \cdots, A_{q-1}$,

$$A_e = (a_{ij}^{(e)}) \quad (0 \leqslant i, j \leqslant q-1, 1 \leqslant e \leqslant q-1).$$

其中

$$a_{ij}^{(e)} = a_e a_i + a_j \in \boldsymbol{F}_q.$$

先证每个 A_e 均是拉丁方. 因若 A_e 的第 i 行有两个元素相同,即有 j 和 j',使得

$$a_e a_i + a_j = a_e a_i + a_j'$$

则 $a_j = a_j'$,从而 $j = j'$. 同样若 A_e 中第 j 列有两个元素相同,即有 i 和 i',使得

$$a_e a_i + a_j = a_e a_i' + a_j.$$

由于$1 \leqslant e \leqslant q-1$,可知 $a_e \neq 0$. 因此由上式又给出 $a_i = a_i'$,于是又有 $i = i'$. 这就表明每个 A_e 均是拉丁方.

再证当$1 \leqslant e < f \leqslant q-1$时,$A_e$ 和 A_f 正交. 因若有方阵的两个位置(i,j)和(i',j'),使得

$$(a_{ij}^{(e)}, a_{ij}^{(f)}) = (a_{i'j'}^{(e)}, a_{i'j'}^{(f)})$$

则 $a_{ij}^{(e)} = a_{i'j'}^{(e)}$, $a_{ij}^{(f)} = a_{i'j'}^{(f)}$,即

$$\begin{cases} a_e a_i + a_j = a_e a_i' + a_j', \\ a_f a_i + a_j = a_f a_i' + a_j', \end{cases}$$

于是$(a_e - a_f)a_i = (a_e - a_f)a_i'$. 由 $e \neq f$ 可知 $a_e \neq a_f$,从而 $a_i = a_i'$,即 $i = i'$. 并且又有 $a_j = a_j'$,即 $j = j'$. 这就表示(i,j)和(i',j')是方阵的同一位置. 即 A_e 和 A_f 是正交的. (对任意$1 \leqslant e < f \leqslant q-1$). 从而如上定义的 $A_1, A_2, \cdots, A_{q-1}$是完备的 q 阶正交拉丁方组.

例 取 $q=4$. $\boldsymbol{F}_4 = \{a_0 = 0, a_1 = 1, a_2 = \alpha, a_3 = \alpha^2 = \alpha + 1\}$,用定理2.2.2的证明中所述方法,可构作出三个彼此正交的4阶拉丁

方 A_1,A_2和 A_3,其中 $A_e=(a_{ij}^{(e)})$,$a_{ij}^{(e)}=a_ea_i+a_j(0\leqslant i,j\leqslant 2)$. 例如对于 A_1:

$$a_{00}^{(1)}=a_1a_0+a_0=0,\quad a_{01}^{(1)}=a_1a_0+a_1=1,$$
$$a_{02}^{(1)}=a_1a_0+a_2=\alpha,\quad a_{03}^{(1)}=\alpha^2.$$
$$a_{10}^{(1)}=a_1a_1+a_0=1,\quad a_{11}^{(1)}=0,\quad a_{12}^{(1)}=1+\alpha=\alpha^2,$$
$$a_{13}^{(1)}=1+\alpha^2=\alpha.$$
$$a_{20}^{(1)}=a_1a_2+a_0=\alpha,\quad a_{21}^{(1)}=\alpha+1=\alpha^2,\quad a_{22}^{(1)}=0,$$
$$a_{23}^{(1)}=\alpha+\alpha^2=1.\quad a_{30}^{(1)}=a_1a_3+a_0=\alpha^2,$$
$$a_{31}^{(1)}=\alpha^2+1=\alpha,\quad a_{32}^{(1)}=\alpha^2+\alpha=1,\quad a_{33}^{(1)}=\alpha^2+\alpha^2=0.$$

从而

$$A_1=\begin{bmatrix}0&1&\alpha&\alpha^2\\1&0&\alpha^2&\alpha\\\alpha&\alpha^2&0&1\\\alpha^2&\alpha&1&0\end{bmatrix}.$$

同样算出

$$A_2=\begin{bmatrix}0&1&\alpha&\alpha^2\\\alpha&\alpha^2&0&1\\\alpha^2&\alpha&1&0\\1&0&\alpha^2&\alpha\end{bmatrix},\quad A_3=\begin{bmatrix}0&1&\alpha&\alpha^2\\\alpha^2&\alpha&1&0\\1&0&\alpha^2&\alpha\\\alpha&\alpha^2&0&1\end{bmatrix}.$$

下一个定理表明完备正交拉丁方组和上节所述有限射影平面有直接联系.

2.2.3 定理 设 $n\geqslant 3$,则存在 n 阶完备正交拉丁方组 $\Longleftrightarrow$ 存在 n 阶射影平面.

证明 设 π 为 n 阶射影平面,l 为 π 中一条直线,l 上的 $n+1$个点为 $P_1,P_2,\cdots,P_{n+1}$,l 外的$(n^2+n+1)-(n+1)=n^2$个点为 $Q_1,\cdots,Q_{n^2}$. 对于每个点 P_j,我们把除了 l 之外过 P_j 的其余 n 条

直线随意标记成1,2,…,n. 现在我们用 a_{ij}表示直线$\overline{Q_iP_j}$的标记.于是得到一个 n^2行$(n+1)$列的长方阵:

$$M=\begin{bmatrix} a_{11}, & a_{12}, & \cdots, & a_{1,n+1} \\ & \cdots\cdots\cdots\cdots & & \\ a_{n^2,1} & a_{n^2,2}, & \cdots, & a_{n^2,n+1} \end{bmatrix}$$

对于这个长方阵的任意两列,例如第 i 列和第 j 列$(1\leqslant i\neq j\leqslant n+1)$,$n^2$个数对$(a_{li},a_{lj})(1\leqslant l\leqslant n^2)$是彼此不同的. 因若$(a_{li},a_{lj})=(a_{l'i},a_{l'j})(l\neq l')$则$\overline{Q_lP_i}=\overline{Q_{l'}P_i}$,$\overline{Q_lP_j}=\overline{Q_{l'}P_j}$. 从而直线$\overline{Q_lQ_{l'}}$既过 P_i 又过 P_j. 于是$\overline{Q_lQ_l'}=l$. 这和 Q_l,Q'_l 均不在 l 上的假定相矛盾.

将 M 的 n^2个行上下顺序作适当调整(即置换),总可得到新的长方阵 M',其前两列有如下形式:

$$M'=\begin{bmatrix} 1 & 1 & \cdots \\ 1 & 2 & \cdots \\ \vdots & \vdots & \\ 1 & n & \\ 2 & 1 & \\ 2 & 2 & \\ \vdots & \vdots & \cdots \\ 2 & n & \\ \vdots & \vdots & \\ n & 1 & \\ n & 2 & \\ \vdots & \vdots & \\ n & n & \cdots \end{bmatrix}$$

由于 M' 的诸行只是 M 中诸行的一个置换,从而 M' 仍有上述性质. 现在把长方阵 M' 后边 $n-1$列的每一列中的 n^2个元素都作成一个 n 阶方阵. 办法是:前 n 个数为第一列,接下来的 n 个

数为第二列，…，最后 n 个数作第 n 列. 利用长方阵 M' 的上述性质不难验证：如此构作出的 $n-1$ 个 n 阶方阵是彼此正交的拉丁方.

现在设 $A_1,\cdots,A_{n-1}$ 是彼此正交的 n 阶拉丁方. 将每个 A_i 拉长成一列，然后将这 $n-1$ 列排在一起，再将上面 M' 的前两列排在它们的最左边，从而得到一个 n^2 行 $(n+1)$ 列的长方阵 $\overline{M}=(a_{ij})(1\leqslant i\leqslant n^2,1\leqslant j\leqslant n+1)$. 这个 $\overline{M}$ 便有上面 M 所具有的性质. 现在我们设想：对应于 $\overline{M}$ 的 n^2 个行，我们分别有 n^2 个点 $Q_1,\cdots,Q_{n^2}$，此外还有 $n+1$ 个点 $P_1,\cdots,P_{n+1}$. 另一方面，对于每个 $k,j(1\leqslant k\leqslant n,1\leqslant j\leqslant n+1)$，我们定义一条直线 l_{kj}，其上的 $n+1$ 个点为 P_j 和 $\{Q_i\mid a_{ij}=k,1\leqslant i\leqslant n^2\}$，除了这 $n(n+1)$ 条直线之外，我们还定义 $P_1,\cdots,P_{n+1}$ 也构成一条直线. 请读者利用长方阵 $\overline{M}$ 的性质证明上面构作出一个 n 阶射影平面(即验证射影平面的三条公理).

由这个定理可知，定理2.1.6与定理2.2.2是等价的. 我们在前面说过，Tarry 证明了不存在一对六阶的正交拉丁方，从而更不存在完备的六阶正交拉丁方组. 于是不存在6阶射影平面. 我们在前面已经具体给出了一对10阶的正交拉丁方. 但是一个10阶射影平面相当于9个彼此正交的10阶拉丁方！由此可见，构作10阶射影平面是相当困难的. 利用前节的 Bruck－Ryser 定理，知道对于 $n=14,21,22,\cdots$，均不存在完备的 n 阶正交拉丁方组. 我们在前面还讲过，当 $n\equiv 2 \pmod 4$，$n\geqslant 10$ 时，均存在一对 n 阶正交拉丁方，构作方法比较复杂. 现在我们证明：对于 $n\not\equiv 2 \pmod 4$ $(n\geqslant 3)$ 的情形，可以很容易构作出一对 n 阶正交拉丁方来.

2.2.4 定理 若存在一对 m 阶正交拉丁方，也存在一对 n

阶正交拉丁方，则必然存在一对 nm 阶正交拉丁方.

证明 构作方法是利用方阵的一种“乘积”，叫作 Kronecker 积. 为了避免使用复杂的数学符号，我们举一个具体例子.

设 A,A' 是一对正交的3阶拉丁方，B,B' 为正交的4阶拉丁方. $A=(a_{ij})(1\leqslant i,j\leqslant 3)$，$B=(b_{ij})$，$1\leqslant i,j\leqslant 4$. 我们用 A 和 B 构作出一个12阶方阵 C，首先我们将它的12行和12列用下面的12个标记来表示：

(1,1)，(1,2)，(1,3)，(1,4)，(2,1)，(2,2)，(2,3)，(2,4)，(3,1)，(3,2)，(3,3)，(3,4). 而12阶方阵 C 中第 (i,j) 行和第 (i',j') 列处的元素为 $\langle a_{ii'},b_{jj'}\rangle$. 我们规定 $\langle a,b\rangle=\langle a',b'\rangle$ 是指 $a=a'$ 同时 $b=b'$. 由于 a 有3个取值，b 有4个取值，从而共有12个元素 $\langle a,b\rangle$. 将方阵 C 的第1行和第1列写出则为

$$
\begin{array}{c}
 \\
(1,1)\\ (1,2)\\ (1,3)\\ (1,4)\\ (2,1)\\ (2,2)\\ (2,3)\\ (2,4)\\ (3,1)\\ (3,2)\\ (3,3)\\ (3,4)
\end{array}
\begin{array}{l}
\quad(1,1)\qquad(1,2)\qquad(1,3)\qquad(1,4)\qquad(2,1)\cdots(2,4)\ (3,1)\cdots(3,4)\\
\left[\begin{array}{llllllll}
\langle a_{11},b_{11}\rangle & \langle a_{11},b_{12}\rangle & \langle a_{11},b_{13}\rangle & \langle a_{11},b_{14}\rangle & \langle a_{12},b_{11}\rangle & \cdots\cdots & & \langle a_{13},b_{14}\rangle\\
\langle a_{11},b_{21}\rangle\cdots & & & & & & & \\
\langle a_{11},b_{31}\rangle\cdots & & & & & & & \\
\langle a_{11},b_{41}\rangle\cdots & & & & (i',j') & & & \\
\langle a_{21},b_{11}\rangle\cdots & & & & \vdots & & & \\
\langle a_{21},b_{21}\rangle\cdots & & & & \vdots & & & \\
\langle a_{21},b_{31}\rangle\cdots & & & (i,j)\cdots\cdots & \langle a_{ii'},b_{jj'}\rangle & & & \\
\langle a_{21},b_{41}\rangle\cdots & & & & & & & \\
\langle a_{31},b_{11}\rangle\cdots & & & & & & & \\
\langle a_{31},b_{21}\rangle\cdots & & & & & & & \\
\langle a_{31},b_{31}\rangle\cdots & & & & & & & \\
\langle a_{31},b_{41}\rangle\cdots & & & & & & &
\end{array}\right]
\end{array}
$$

由 A 和 B 均为拉丁方，可知上面方阵 C 的第一列恰好为12个不同的元素 $\langle a,b\rangle$. 同理知其余诸列和诸行也是如此. 从而 C 为12

阶拉丁方.我们再用同样办法由 A' 和 B' 构作出另一个12阶拉丁方 C'.由 A 与 A' 正交和 B 与 B' 正交可以证明 C 与 C' 是正交的.

2.2.5 定理 当 $n\geqslant 3, n\not\equiv 2 \pmod 4$ 时,均存在一对正交的 n 阶拉丁方.

证明 设 $n=2^{a_0}p_1^{a_1}\cdots p_s^{a_s}$ 是 n 的素因子分解式,其中 $p_1,\cdots,p_s$ 是奇素数.$a_1,\cdots,a_s\geqslant 1$.由 $n\not\equiv 2 \pmod 4$ 可知 $a_0=0$ 或者 $a_0\geqslant 2$.由定理2.2.2可知当 $a_0\geqslant 2$ 时,存在一对 2^{a_0} 阶正交拉丁方.并且也存在一对 $p_i^{a_i}$ 阶正交 拉丁方($1\leqslant i\leqslant s$).再由定理2.2.4即知存在一对 n 阶正交拉丁方.证毕.

将定理2.2.5和 Bose 的结果合并起来,便知对每个 $n\geqslant 3$($n\neq 6$),均存在一对正交的 n 阶拉丁方.但是对每个不是素数幂的 n,彼此正交的 n 阶拉丁方最大个数问题是一个未完全解决的问题.我国数论学家王元、陆鸣皋等人对它的上界曾作过好的估计.

2.2.6 习 题

1. 构作4个彼此正交的5阶拉丁方.
2. 设 $L^{(k)}=(a_{ij}^{(k)})$ 为9阶方阵,($1\leqslant i,j\leqslant 9$).其中 $a_{ij}^{(k)}\equiv i+jk \pmod 9$,$0\leqslant a_{ij}^{(k)}\leqslant 8$.

   试问 $L^{(k)}$($1\leqslant k\leqslant 8$)当中哪些是拉丁方?$L^{(2)}$ 和 $L^{(5)}$ 是否正交?$L^{(4)}$ 和 $L^{(5)}$ 是否正交?
3. 若存在 a 个彼此正交的 m 阶拉丁方,又存在 b 个彼此正交的 n 阶拉丁方,则必存在 $\min(a,b)$ 个彼此正交的 mn 阶拉丁方.其中 $\min(a,b)$ 表示 a 和 b 当中最小的数.

§ 2.3　区组设计

假设某种农作物的栽培依赖于 k 个因素(水份，土壤，肥料，…)，每个因素有 v 种选择，我们想研究各种因素对农作物生长的影响. 如果将各种因素的各种选择均试验一次，就需要试验 v^k 次. 这个数目往往太大，所以通常要求设计一些试验次数 b 较小的方案，使得各种因素均衡地组合，以看出各种因素的影响和它们之间的相互影响. 上节的正交拉丁方可用来设计这种试验方案. 而多数试验方案是藉助于下面的组合构图.

2.3.1　定义　设 $X=\{x_1,\cdots,x_v\}$ 是一个 v 元集合，$X_1,\cdots X_b$ 是 X 的 b 个不同的子集. 称这 b 个子集组成一个参数为 (b,v,k,r) 的组合构图，是指满足以下两个条件(今后用 $|S|$ 表示集合 S 中元素个数)：

(1) $|X_i|=k(1\leqslant i\leqslant b)$，即每个 X_i 都是 k 元子集.

(2) 每个 x_i 都恰好在 r 个 X_j 之中 $(1\leqslant i\leqslant v)$.

每个子集 X_j 叫作是一个区组(Block)，每个元素 x_i 叫作是一个品种(Variety).

由于每个区组均有 k 个品种，从而 b 个区组 $X_1,\cdots,X_b$ 中一共包含 bk 个品种. 但是 X 的 v 个品种之中的每个 x_i 都恰好在 $X_1,X_2,\cdots,X_b$ 中出现 r 次. 所以我们得到参数之间的关系

$$vr = bk. \tag{1}$$

如果 $v=b$(从而 $k=r$)，则叫作参数为 (v,k) 的对称组合构图.

例　设 X 是射影平面 $\pi(F_q)$ 的 $q^2+q+1=v$ 个点构成的集

合，每个点是一个品种. 而每条直线是一个区组. 由于每条直线均恰好有 $q+1=k$ 个点，每个点都恰好在 $q+1=r$ 个直线上. 从而这是一个对称的组合构图，参数为

$$b=v=q^2+q+1, k=r=q+1.$$

我们可以用有限域来构作其他参数的组合构图. 办法是采用更高维数的射影空间. 这些射影空间可以象二维的射影平面那样类似地定义. 设 n 是自然数，F 为任意的域，考虑集合

$$S=\{(a_0,a_1,\cdots,a_n)\,|\,a_i\in F\},(a_0,\cdots,a_n)\neq(0,\cdots,0)\}$$

在集合 S 中定义一个等价关系：称 $(a_0,a_1,\cdots,a_n)$ 和 $(b_0,b_1,\cdots,b_n)$ 等价，是指存在 $\alpha\in F^*$，使得

$$\alpha b_i=a_i(0\leqslant i\leqslant n)，即 (a_0,a_1,\cdots,a_n)=\alpha(b_0,b_1,\cdots,b_n).$$

每个等价类记成 $[a_0,a_1,\cdots,a_n]$. 所有这样的等价类组成的集合 $P^n(F)$ 叫作域 F 上的 **n维射影空间**. 当 $n=2$时，$P^2(F)$ 就是域 F 上的射影平面.

$P^n(F)$ 中每个元素 $[a_0,a_1,\cdots,a_n]$ 叫作一个**点**，当 F 为有限域 F_q 时，集合 S 共有 $q^{n+1}-1$个元素，而每 $q-1$个元素形成一个等价类，从而 $P^n(F_q)$ 中共有 $\frac{q^{n+1}-1}{q-1}=q^n+q^{n-1}+\cdots+q+1$个点.

考虑域 F 上的 $n-k$ 个方程($1\leqslant k\leqslant n$)构成的线性方程组：

$$\begin{cases}a_{10}x_0+\cdots+a_{1n}x_n=0,\\ a_{20}x_0+\cdots+a_{2n}x_n=0,\\ \cdots\cdots\\ a_{n-k,0}x_0+\cdots+a_{n-k,n}x_n=0,\end{cases}\qquad(*)$$

其中 $a_{ij}\in F(1\leqslant i\leqslant n-k,0\leqslant j\leqslant n)$. 并且设这个方程组当中的任何一个方程都不是多余的，即都不能由其余 $n-k-1$个方程推出来，这样的方程组叫作是**线性无关**的. 例如方程组

$$\begin{cases} x_0 + \quad\quad x_2 = 0, \\ \quad\quad 2x_1 + x_2 = 0, \\ 2x_0 - 2x_1 + x_2 = 0 \end{cases}$$

不是线性无关的，因为将第一个方程两边乘以2再分别减去第二个方程的两边，便得到第三个方程，所以它相当于前两个方程组成的方程组，即第三个方程是多余的.

现在设（*）是线性无关的方程组. 若$(x_0,\cdots,x_n)$是它在域F中的一组解，则对每个$\alpha\in F^*$，易知$\alpha(x_0,\cdots,x_n)=(\alpha x_0,\cdots,\alpha x_n)$也是（*）的一组解. 从而可以谈射影空间$P^n(F)$中的点$[x_0,\cdots,x_n]$是方程组（*）的解（其中$x_0,\cdots,x_n$不全为零）. 由于$(x_0,\cdots,x_n)$共有$n+1$个分量，即有$n+1$个自由度（或叫维数）. 加了一个等价条件之后变成$[x_0,\cdots,x_n]$，从而射影空间$P^n(F)$有$(n+1)-1=n$个自由度（这就是为什么称作$n$维射影空间）. 如果$[x_0,\cdots,x_n]$又是线性无关的方程组（*）的解，由于这个方程组对解给出$n-k$个限制，所以解的自由度为$n-(n-k)=k$. 因此，我们把由$n-k$个方程组成的线性无关方程组（*）在$P^n(F)$中的全部解$[x_0,\cdots,x_{n+1}]$构成的集合，叫作$P^n(F)$的一个**k维线性簇**.

设F为有限域F_q. 先将（*）看成是

$$V = \{(x_0,\cdots,x_n) \mid x_i \in F\}$$

上的方程组. 由于V是$n+1$维的，从而方程组（*）的解是$(n+1)-(n-k)=k+1$维的. 所以非零解共有$q^{k+1}-1$个. 每$q-1$个解组成一个等价类. 因此，n维射影空间$P^n(F_q)$中每个k维线性簇均有$\dfrac{q^{k+1}-1}{q-1}=q^k+q^{k-1}+\cdots+q+1$个点.

为了书写方便，我们引入记号

$$[q^n]_k = (q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{k-1})(1\leqslant k\leqslant n).$$

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{[q^n]_k}{[q^k]_k}.$$

利用简单的线性代数知识，可以证明：

(1) n 维射影空间 $P^n(F_q)$ 的每个点均恰好在 $\begin{bmatrix} n \\ k \end{bmatrix}_q$ 个 k 维线性簇之中.

(2) $P^n(F_q)$ 中一共有 $\begin{bmatrix} n+1 \\ k+1 \end{bmatrix}_q$ 个 k 维线性簇. 因此，若把 $P^n(F_q)$ 中的每个点看作是一个品种，把它的每个 l 维线性簇看作是一个区组. 由上面的计数即知我们对每个 $1 \leqslant l \leqslant n$，给出一个组合构图，其参数为 $b = \begin{bmatrix} n+1 \\ l+1 \end{bmatrix}_q$ (l 维线性簇个数)，$v = \begin{bmatrix} n+1 \\ 1 \end{bmatrix}_q = \dfrac{q^{n+1}-1}{q-1}$ (点的个数)，$k = \begin{bmatrix} l+1 \\ 1 \end{bmatrix}_q = \dfrac{q^{l+1}-1}{q-1}$ (每个线性簇中的点数). $r = \dfrac{bk}{v} = \begin{bmatrix} n \\ l \end{bmatrix}_q$ (包含某个点的 k 维线性簇个数).

射影空间 $P^n(F)$ 中的每个点 $[a_0, a_1, \cdots, a_n]$ 是一个0维线性簇，因为它是 n 个线性无关方程

$$\begin{cases} a_1 x_0 - a_0 x_1 = 0, \\ a_2 x_0 - a_0 x_2 = 0, \\ \quad \vdots \\ a_n x_0 - a_0 x_n = 0 \end{cases}$$

的全部解. 现在我们还可以构作更一般的设计方案. 设 $0 \leqslant m \leqslant l \leqslant n$. 我们用 X 表示 $P^n(F_q)$ 中所有 m 维线性簇构成的集合，每个 m 维线性簇是一个品种. 而 $P^n(F_q)$ 中每个 l 维线性簇看作是一个区组 X_j，注意，这时我们不是把 X_j 看作是 $P^n(F_q)$ 中的点组成的集合，而是把 X_j 看成是 X 的子集，即看成是由包含在 X_j 中的所有 m 维线性簇构成的集合. 利用线性代数可以证明这样也

构成一个组合构图，其参数为

$$b=\begin{bmatrix}n+1\\l+1\end{bmatrix}_q \quad (P^n(F_q)\text{中 } l \text{ 维线性簇个数}).$$

$$v=\begin{bmatrix}n+1\\m+1\end{bmatrix}_q \quad (P^n(F_q)\text{中 } m \text{ 维线性簇个数}).$$

$$k=\begin{bmatrix}l+1\\m+1\end{bmatrix}_q \quad (\text{每个 } l \text{ 维线性簇包含的 } k \text{ 维线性簇个数}).$$

$$r=\frac{bk}{v}=\begin{bmatrix}n-m\\l-m\end{bmatrix}_q \quad (\text{包含一个固定的 } k \text{ 维线性簇的 } l \text{ 维线性簇个数}).$$

当取 $m=0$时（即品种取成点时），就是前面给出的组合构图.

组合构图只是考虑了各种因素的均衡选择. 假如还要考虑不同因素之间交叉影响，便有如下的试验设计方案.

2.3.2 定义 一个参数为(b,v,k,r)的组合构图叫作是不完全平衡区组设计(Balanced imcomplete block design，简记为BIBD)，是指 $v\geqslant k\geqslant 2$，并且对 X 中任意两个不同的品种 x_i 和 x_j，均恰好同时出现在 λ 个区组 X_j 之中.

包含品种 x_1的区组共有 r 个，而对于这每个区组，x_1都与区组中另外 $k-1$个品种共处于此区组中. 另一方面，对于除了 x_1 之外的所有 $v-1$个其他品种，由定义 x_1恰好与它们之中的每一个品种共处于 λ 个区组中. 于是

$$r(k-1)=\lambda(v-1) \tag{2}$$

由(2)式和(1)式中的 $bk=rv$ 可知，b 和 r 由参数 v,k,λ 所决定. 所以通常对于 BIBD 只列出参数 v,k,λ. 当 $b=v$(从而 $k=r$)时，BIBD 也叫作是对称的. 此时 $k(k-1)=\lambda(v-1)$.

例1 令 $X=\{0,1,2,3,4,5,6\}=F_7$. $x_0=\{0,1,3\}$，而 $X_i=X_0+i=\{i,1+i,3+i\}(0\leqslant i\leqslant 6)$，即7个区组为

$$X_0=\{013\},X_1=\{124\},X_2=\{235\},X_3=\{346\},$$
$$X_4=\{450\},X_5=\{561\},X_6=\{602\},$$

这是一个对称的 BIBD，其参数为

$b=v=7$（7个品种，7个区组）

$k=r=3$（每区组有3个品种，每品种在3个区组之中）

$\lambda=1$ （任意两个不同品种均恰好同时在一个区组之中）.

现在我们用有限域上的射影空间来构作 BIBD.

例2 取 $X=\pi(\boldsymbol{F}_q)=\boldsymbol{P}^2(\boldsymbol{F}_q)$ 为 $\boldsymbol{F}_q$ 上的射影平面，$\boldsymbol{P}^2(\boldsymbol{F}_q)$ 中每点为品种，每条直线为一个区组. 我们知道由此构成一个组合构图，参数为 $b=v=q^2+q+1$，$k=r=q+1$. 由于任意两个不同的点均恰好在一条直线上，因此这实际上是一个 BIBD，其中 $\lambda=1$.

更一般地，对每个 $n\geqslant 2$，$1\leqslant t\leqslant n-1$. 取 n 维射影空间 $\boldsymbol{P}^n(\boldsymbol{F}_q)$ 中的点作为品种，每个 t 维线性簇作为区组. 由前述我们知道这是一个组合构图，其参数为

$$b=\begin{bmatrix} n+1 \\ t+1 \end{bmatrix}_q \quad (\boldsymbol{P}^n(\boldsymbol{F}_q)\text{中 } t \text{ 维线性簇个数})$$

$$v=\begin{bmatrix} n+1 \\ 1 \end{bmatrix}_q \quad (\boldsymbol{P}^n(\boldsymbol{F}_q)\text{中点数})$$

$$k=\begin{bmatrix} t+1 \\ 1 \end{bmatrix}_q \quad (\text{每个 } t \text{ 维线性簇中点数})$$

$$r=\begin{bmatrix} n \\ t \end{bmatrix}_q \quad (\text{包含某固定点的 } t \text{ 维线性簇个数})$$

进而，对于 $\boldsymbol{P}^2(\boldsymbol{F}_q)$ 中任意两个不同的点 $P=[a_0,a_1,\cdots,a_n]$ 和 Q

$=[b_0,b_1,\cdots,b_n]$，有唯一的1维线性簇(直线)

$$\overline{PQ}=\{\lambda(a_0,\cdots,a_n)+\mu(b_0,\cdots,b_n)\mid\lambda,\mu\in \boldsymbol{F}_q,\lambda\text{ 和 }\mu\text{ 不同时为}0\}.$$

同时包含点 P(取 $\lambda=1,\mu=0$)和点 Q(取 $\lambda=0,\mu=1$). 并且一个 t 维线性簇同时包含点 P 和 Q，则必包含直线$\overline{PQ}$. 而包含直线$\overline{PQ}$的 t 维线性簇共有$\begin{bmatrix}n-1\\t-1\end{bmatrix}_q$个. 因此上述组合构图事实上是一个 BIBD，其中 $\lambda=\begin{bmatrix}n-1\\t-1\end{bmatrix}_q$.

特别取 $t=n-1$，即取所有 $n-1$维线性簇作为区组，便得到对称的 BIBD，其参数为

$$b=v=\begin{bmatrix}n+1\\n\end{bmatrix}_q=\begin{bmatrix}n+1\\1\end{bmatrix}_q=\frac{q^{n+1}-1}{q-1},$$

$$r=k=\begin{bmatrix}n\\n-1\end{bmatrix}_q=\begin{bmatrix}n\\1\end{bmatrix}_q=\frac{q^n-1}{q-1},$$

$$\lambda=\begin{bmatrix}n-1\\n-2\end{bmatrix}_q=\begin{bmatrix}n-1\\1\end{bmatrix}_q=\frac{q^{n-1}-1}{q-1}.$$

例3 现在我们改用 $\boldsymbol{F}_q$ 上的仿射空间. 对于 $n\geqslant 2$，$\boldsymbol{F}_q$ 上的 n 维仿射空间是指集合

$$\boldsymbol{A}^n(\boldsymbol{F}_q)=\{(a_1,a_2,\cdots,a_n)\mid a_i\in \boldsymbol{F}_q\}.$$

于是它共有 q^n 个元素，每个元素叫作 $\boldsymbol{A}^n(\boldsymbol{F}_q)$的一个点. 满足 $n-k$个线性无关方程

$$\begin{cases}a_{11}x_1+\cdots+a_{1n}x_n=0,\\ \cdots\cdots\\ a_{n-k,1}x_1+\cdots+a_{n-k,n}x_n=0\end{cases}\qquad(a_{ij}\in \boldsymbol{F}_q)$$

的全部点组成的集合叫作 $\boldsymbol{A}^n(\boldsymbol{F}_q)$的一个 k 维子空间. 可以证明：每个 k 维子空间有 q^k 个点. 如果取 $X=\boldsymbol{A}^n(\boldsymbol{F}_q)$，$1\leqslant t\leqslant n-1$. 每

个点作为品种，每个 t 维子空间作为区组. 由此可得到一个 BIBD，并且利用线性代数可以计算出其参数为

$$b=q^{n-t}\begin{bmatrix} n \\ t \end{bmatrix}_q \quad (A^n(F_q)\text{中 } t \text{ 维子空间个数}).$$

$$v=q^n \quad (A^n(F_q)\text{中点数})$$

$$r=\begin{bmatrix} n \\ t \end{bmatrix}_q \quad (\text{包含某固定点的 } t \text{ 维子空间个数}).$$

$$k=q^t \quad (t \text{ 维子空间中的点数}).$$

$$\lambda=\begin{bmatrix} n-1 \\ t-1 \end{bmatrix}_q \quad (\text{包含两个不同点 } P \text{ 和 } Q \text{ 的 } t \text{ 维子空间的个数}).$$

利用有限域上其他几何（辛几何，酉几何，正交几何等），还可以构作出更多的 BIBD. 有兴趣的读者可参看万哲先等著《有限几何和区组设计》一书.

2.3.3 习 题

1. 设 X 的 b 个子集 $X_1,\cdots,X_b$ 构成一个参数为 (v,k,λ) 的 BIBD，令 $Y_i=X-X_i$（X_i 在 X 中的补集）$(1\leqslant i\leqslant b)$. 求证 $Y_1,\cdots,Y_b$ 也构成一个 BIBD. 试计算这个 BIBD 的参数.
2. 设 $v>3$. 则参数为 $(v,k,\lambda)=(v,3,1)$ 的 BIBD 叫作一个 v 阶的 Steiner 三元系. 求证：若存在 v 阶的 Steiner 三元系，则必然 $b=\frac{1}{6}v(v-1)$，$r=\frac{1}{2}(v-1)$，并且 $v\equiv 1$ 或 $3 \pmod 6$.（注记：早在1859年，Reiss 对于 $v\equiv 1$ 或 $3 \pmod 6$ 的每个 $v>3$，均构作出 v 阶 Steiner 三元系）
3. 试构作一个具体的7阶 Steiner 三元系.
4. 试构作一个对称的 BIBD，其参数为 $(v,k,\lambda)=(13,4,1)$.

§2.4 差集合

2.4.1 定义 设 $d_1,d_2,\cdots,d_k$ 是 k 个整数. $k\geqslant 2$, v 为正整数, $v\geqslant 2$. 令

$$S=\{d_i-d_j \mid 1\leqslant i,j\leqslant k, i\neq j\},$$

如果对每个 $a(1\leqslant a\leqslant v-1)$, S 的 $k(k-1)$ 个数中均恰好有 λ 个模 v 同余于 a, 就称 $D=\{d_1,d_2,\cdots,d_k\}$ 是一个参数为 (v,k,λ) 的**差集合**.

例1 取 $v=7, k=3, \lambda=1, D=\{0,1,3\}$. 则模7的意义下集合 S 为

$$\begin{aligned}S&=\{0-1=6,0-3=4,1-3=5,1-0=1,3-0=3,\\&\quad 3-1=2\}\\&=\{6,4,5,1,3,2\},\end{aligned}$$

从而 D 是一个参数为 $(7,3,1)$ 的差集合.

2.4.2 定理 $D=\{d_1,d_2,\cdots,d_k\}$ 为参数 (v,k,λ) 的差集合 $\Longleftrightarrow$ X 的 v 个子集 $D,1+D,2+D,\cdots,(v-1)+D$ 构成参数为 (v,k,λ) 的对称 BIBD. 这里 X 是 v 个模 v 同余类所组成的集合, 而 $i+D=\{i+d_1,\cdots,i+d_k\}$.

证明 设 $D=\{d_1,\cdots,d_k\}$ 是参数 (v,k,λ) 的差集合. 则每个区组 $D+l(0\leqslant l\leqslant v-1)$ 均是 $X=\{0,1,\cdots,v-1\}$ 的 k 元子集. 并且每个整数 a(模 v)恰好在 k 个区组 $D+(a-d_i)(1\leqslant i\leqslant k)$ 之中. 又对于任意两个整数 a 和 b, $a\not\equiv b(\mathrm{mod}\ v)$. 若 a 和 b 同时在 $D+l$ 中, 则有 i,j, $1\leqslant i\neq j\leqslant k$, 使得 $d_i+l\equiv a$, $d_j+l\equiv b(\mathrm{mod}\ v)$. 于是 $d_i-d_j\equiv a-b\not\equiv 0(\mathrm{mod}\ v)$. 由于 D 是差集合, 可知共有 λ 个 (i,j)

满足 $d_i-d_j\equiv a-b \pmod v$. 而对于每组这样的$(i,j)$，满足 $d_i+l\equiv a, d_j+l\equiv b \pmod v$的 l 是唯一决定的. 因此 a 和 b 同时在 λ 个区组 $D+l$ 中. 即 $D+l(0\leqslant l\leqslant v-1)$是参数$(v,k,\lambda)$的对称 BIBD. 反之，类似可证：若 $D+l(0\leqslant l\leqslant v-1)$是参数$(v,k,\lambda)$的对称 BIBD，则 D 是参数(v,k,λ)的差集合.

根据定理2.4.2，差集合相当于一类特殊的对称 BIBD，因此差集合的要求更强. 由定理2.4.2还可知道，差集合的三个参数满足条件：$k(k-1)=\lambda(v-1)$. 现在我们用有限域构作差集合.

2.4.3 定理 当 $q=p^n$ 时(p 为素数，$n\geqslant 1$)，则存在参数为$(v,k,\lambda)=(q^2+q+1,q+1,1)$的差集合.

证明 取 F_{q^3}中一个本原元素 α，则 $\alpha^v=\alpha^{\frac{q^3-1}{q-1}}$是 F_q 的本原元素$(v=q^2+q+1)$. 并且 $F_{q^3}^*=\{1,\alpha,\cdots,\alpha^{q^3-2}\}$. 由于 α 是 $F_q[x]$中3次不可约多项式的根. 从而 F_{q^3}中每个元素 α^i 可唯一表成

$$\alpha^i=a_0+a_1\alpha+a_2\alpha^2,\quad a_i\in F_q.$$

我们把这个元素记成(a_0,a_1,a_2)，并且以 α^i 表示射影平面$P^2(F_q)$中的点$[a_0,a_1,a_2]$，若

$$\alpha^j=b_0+b_1\alpha+b_2\alpha^2,\quad b_i\in F_q.$$

则： α^i 和 α^j 是 $P^2(F_q)$中同一个点

$\Longleftrightarrow [a_0,a_1,a_2]=[b_0,b_1,b_2]$

$\Longleftrightarrow$有 $\beta\in F_q^*$，使得 $a_i=\beta b_i \quad (i=0,1,2)$.

$\Longleftrightarrow$有 $\beta\in F_q^*=\{1,\alpha^v,\alpha^{2v},\cdots,\alpha^{(q-2)v}\}$，使 $\alpha^i=\beta\alpha^j$

$\Longleftrightarrow i\equiv j \pmod v$.

由此可知，$1,\alpha,\alpha^2,\cdots,\alpha^{v-1}$就是射影平面 $P^2(F_q)$中全部 $v=q^2+q+1$个不同的点.

用 L 表示过点$1=[1,0,0]$和点 $\alpha=[0,1,0]$的直线. 于是 L 由 $k=q+1$个点组成,从而 $L=\{\alpha^{d_1},\alpha^{d_2},\cdots,\alpha^{d_k}\}$其中$0\leqslant d_i\leqslant v-1$. 我们现在来证 $D=\{d_1,d_2,\cdots,d_k\}$就是参数为$(v,k,1)$的差集合.

首先,设 α^i 和 α^j 是 $P^2(F_q)$中两个不同的点,l 为过这两点的直线. 那末 l 中点都有形式

$$A\alpha^i+B\alpha^j \qquad (A,B\in F_q, A \text{ 和 } B \text{ 不全为零}). \qquad (*)$$

这是因为若 $\alpha^i=(c_0,c_1,c_2)$,$\alpha^j=(b_0,b_1,b_2)$,$c_i,b_i\in F_q$,那末当直线 l 是$\langle x_0,x_1,x_2\rangle$,即由方程 $a_0x_0+a_1x_1+a_2x_2=0$所定义时,则 α^i 和 α^j 在 l 上相当于说它们满足此方程,即

$$c_0x_0+c_1x_1+c_2x_2=0, \qquad b_0x_0+b_1x_1+b_2x_2=0.$$

于是 $A(c_0,c_1,c_2)+B(b_0,b_1,b_2)=A\alpha^i+B\alpha^j$ 也满足 l 的方程. 当 A 和 B 不全为零时,$A\alpha^i+B\alpha^j\neq 0=(0,0,0)$. 否则 $A\alpha^i=-B\alpha^j$,由于 $A,B\in F_q$,于是 α^i 和 α^j 为 $P^2(F_q)$中同一点. 这与假设矛盾. 所以 A 和 B 不全为零时,$A\alpha^i+B\alpha^j$ 为直线上的点. A 和 B 的选取共有 q^2-1个可能. 并且当且仅当$(A,B)=c(A',B')$$(c\in F_q^*)$时,$A\alpha^i+B\alpha^j=c(A'\alpha^i+B'\alpha^j)$才和 $A'\alpha^i+B'\alpha^j$ 表示同一个点. 因此$(*)$式共给出直线 l 上$\frac{q^2-1}{q-1}=q+1$个不同的点. 从而$(*)$给出了直线 l 的全部点.

现在,L 是由1和 α 两个点决定的直线,从而 L 中点表示成 $A+B\alpha$($A,B\in F_q$,A 和 B 不全为零),那末对每个$0\leqslant j\leqslant v-1$,$\alpha^j$ 和 α^{j+1}是两个不同的点. 它们决定直线中的点表示成 $A\alpha^j+B\alpha^{j+1}=\alpha^j(A+B\alpha)$. 即 L 中每个点乘以 α^j. 因此

$$\alpha^jL=\{\alpha^j\gamma\mid\gamma\in L\}=\{\alpha^{d_1+j},\alpha^{d_2+j},\cdots,\alpha^{d_k+j}\}\ (0\leqslant j\leqslant v-1)$$

也都是直线. 我们现在来证明这 v 条直线 $\alpha^jL$$(0\leqslant j\leqslant v-1)$两两不同.

我们以 r 表示满足 $\alpha^r L=L$ 的最小正整数. 用除法算式可知，对每个整数 n，$\alpha^n L=L \Longleftrightarrow r|n$. 由于对每个点 P，$\alpha^v P=P$(是射影平面 $P^2(F_q)$ 中同一个点)，于是 $\alpha^v L=L$(因为 α^v 将 L 的每点不变，当然将 L 变成 L). 于是 $r|v$. 另一方面，对 L 中每个点 P，

$$(\alpha^r)^\lambda P = P \Longleftrightarrow \alpha^{\lambda r} \in F_q^* \Longleftrightarrow v|\lambda r.$$

从而使 $(\alpha^r)^\lambda P=P$ 的最小正整数 λ 即为满足 $v|\lambda r$ 的最小正整数 λ，而后者与点 P 无关. 这就表明对于 L 中每个点 P，都给出 L 中 λ 个不同的点 $P,\alpha^r P,\alpha^{2r}P,\cdots,\alpha^{(\lambda-1)r}P$. 如果 L 中还有点 Q，那末又得到 L 中另外 λ 个点 $Q,\alpha^r Q,\cdots,\alpha^{(\lambda-1)r}Q$. 于是 L 中总点数 $k=q+1$是 λ 的倍数. 由此可知 $v|\lambda r|kr$. 但是 $v=q^2+q+1$和 $k=q+1$互素，这表明 $v|r$. 由上面已证 $r|v$，从而 $r=v$. 根据 r 的定义便知 $L,\alpha L,\alpha^2 L,\cdots,\alpha^{v-1}L$ 是射影平面 $P^2(F_q)$中 v 个不同的直线. 由于 $P^2(F_q)$中共有 v 条直线，从而

$$\alpha^j L=\{\alpha^{d_1+j},\alpha^{d_2+j},\cdots,\alpha^{d_k+j}\} \qquad (0\leqslant j\leqslant v-1)$$

便是 $P^2(F_q)$中全部直线. 由上节的例2，它们构成参数为 $(v,k,1)$ 的对称 BIBD. 改用元素的指数(看作模 v 的整数)，便知

$$D+j=\{d_1+j,d_2+j,\cdots,d_k+j\} \qquad (0\leqslant j\leqslant v-1)$$

是参数为 $(v,k,1)$的对称 BIBD. 再由定理2.4.2就知 $D=\{d_1,d_2,\cdots,d_k\}$ 是参数 $(v,k,1)$的差集合.

例2 在定理2.4.3中取 $q=3$，则 $v=13,k=4$. 取 $F_3[x]$中三次本原多项式 x^3+2x+1，令 α 为它的一个根. 则 $F_{27}=F_3(\alpha)$，$\alpha^3=\alpha+2$，而 F_{27}^*中所有元素为

$1=(001)$，	$\alpha^6=(111)$，	$\alpha^{12}=(102)$，
$\alpha=(010)$，	$\alpha^7=(122)$，	$\alpha^{13}=(002)=-1$，
$\alpha^2=(100)$，	$\alpha^8=(202)$，	$\alpha^{14}=-\alpha$，

$\alpha^3=(012)$, $\alpha^9=(011)$, ⋮

$\alpha^4=(120)$, $\alpha^{10}=(110)$, ⋮

$\alpha^5=(212)$, $\alpha^{11}=(112)$, $\alpha^{25}=-\alpha^{12}$.

可取 $\alpha^i(0\leqslant i\leqslant 12)$ 为 $P^2(F_3)$ 中13个点. 由点1和 α 决定的直线 L 上共有4个点，它们是

$$1,\ \alpha,\ 1+\alpha=(011)=\alpha^9 \text{ 和 } 1-\alpha=(021)=-\alpha^3.$$

而在 $P^2(F_3)$ 中 $-\alpha^3$ 和 α^3 是同一个点. 于是 $L=\{1,\alpha,\alpha^3,\alpha^9\}$. 即 $D=\{0,1,3,9\}$ 是以 $(v,k,\lambda)=(13,4,1)$ 为参数的差集合.

将定理2.4.3加以推广，即用一般的 n 维射影空间 $P^n(F_q)$ 代替 $P^2(F_q)$，用 $P^n(F_q)$ 中 $n-1$ 维线性簇(叫作**超平面**)代替 $P^2(F_q)$ 中的一维线性簇(即直线)，便得到如下的著名结果

2.4.4 定理 (Singer, 1938). 设 $q=p^m$, $n\geqslant 2$. 则存在参数 $(v,k,\lambda)=\left(\dfrac{q^{n+1}-1}{q-1},\dfrac{q^n-1}{q-1},\dfrac{q^{n-1}-1}{q-1}\right)$ 的差集合.

证明 取 $F_{q^{n+1}}$ 中一个本原元素 α，则 $F^*_{q^{n+1}}$ 中元素为

$$\alpha^i=a_0\alpha^n+a_1\alpha^{n-1}+\cdots+a_n=(a_0,a_1,\cdots,a_n),\quad a_\lambda\in F_q$$

$(0\leqslant i\leqslant q^{n+1}-2)$. 与定理2.4.3(即 $n=2$ 的情形)一样证明：可以用 $1,\alpha,\cdots,\alpha^{v-1}$ 来表示 n 维射影空间 $P^n(F_q)$ 的 v 个点. 由其中点 $1,\alpha,\cdots,\alpha^{n-1}$ 决定一个超平面

$$K=\{[a_0,a_1,\cdots,a_n]\in P^n(F_q)\,|\,a_0=0\}$$
$$=a_1\alpha^{n-1}+a_2\alpha^{n-2}+\cdots+a_n$$
$$(a_i\in F_q,a_1,\cdots,a_n \text{ 不全为零})$$

由此即知 $\alpha^jK(0\leqslant j\leqslant v-1)$ 也都是 $P^n(F_q)$ 的超平面. 并且可象定理2.4.3一样证明它们是两两不同的. 从而为 $P^n(F_q)$ 中全部 v 个超平面. 由第2.3节例2的最后所述，$\alpha^jK(0\leqslant j\leqslant v-1)$ 是参数为 (v,k,λ) 的对称 BIBD. 令 $K=\{\alpha^{d_1},\cdots,\alpha^{d_k}\}$($d_i$ 是模 v 的整数)，

则 $\alpha^j K=\{\alpha^{d_1+j},\cdots,\alpha^{d_k+j}\}(0\leqslant j\leqslant v-1)$. 由定理2.4.2即知$\{d_1,\cdots,d_k\}$是参数为$(v,k,\lambda)$的差集合. 证毕.

例3 取 $q=2,n=3$. 我们在第1.4节例2中构作了 $F_{16}=F_2(\gamma)$,其中 γ 是 F_{16}的本原元素,$\gamma^4=\gamma^3+1$. F_{16}^*的元素如第1.4节例2所示. $P^3(F_2)$中由$1,\gamma,\gamma^2$决定的超平面共有 $k=7$个元素,它们是$1,\gamma,\gamma^2,1+\gamma=\gamma^{12},1+\gamma^2=\gamma^9,\gamma+\gamma^2=\gamma^{13}$和$1+\gamma+\gamma^2=\gamma^7$,从而$\{0,1,2,7,9,12,13\}$是参数为$(v,k,\lambda)=(15,7,3)$的差集合.

我们在下一节(定理2.5.6)中还要给出构作差集合的一种方法.

2.4.5 习 题

1. 设 $D=\{d_1,d_2,\cdots,d_k\}$是参数为(v,k,λ)的差集合. 求证:(Ⅰ)对每个 $j\in Z$,$D+j=\{d_1+j,\cdots,d_k+j\}$也是同样参数的差集合.
   (Ⅱ)对每个与 v 互素的整数 n,$nD=\{nd_1,\cdots,nd_k\}$也是同样参数的差集合.
2. 试构作参数为$(v,k,\lambda)=(31,6,1)$和$(40,13,4)$的差集合.
3. 设 $D=\{d_1,d_2,\cdots,d_k\}$是参数为(v,k,λ)的差集合,$0\leqslant d_i\leqslant v-1$. 求证 D 在$\{0,1,\cdots,v-1\}$中的补集也是模 v 的差集合. 试计算这个差集合的参数.

§2.5 阿达玛方阵

2.5.1 定义 设 H_n 是 n 阶方阵

$$H_n=(a_{ij})=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ & \cdots\cdots\cdots & & \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

其中每个 a_{ij} 等于1或-1，方阵中第 j 行$(a_{j1},a_{j2},\cdots,a_{jn})$和第 i 行$(a_{i1},a_{i2},\cdots,a_{in})$的内积，指的是实数

$$a_{j1}a_{i1}+a_{j2}a_{i2}+\cdots+a_{jn}a_{in}=\sum_{k=1}^{n}a_{jk}a_{ik}.$$

由于 $a_{ij}=\pm1$，从而每行和自己的内积一定为 n. 如果两行的内积为零，称这两行正交. 如果 H_n 中任意两个不同的行均正交，则称 H_n 为 n 阶阿达玛(Hadamard)阵.

注记 (1) 类似地可以定义 H_n 中两列的内积和正交性. 利用线性代数可知，阿达玛阵的任意两个不同的列也是正交的. 因为：由方阵的乘法易知：H_n 为阿达玛阵$\Longleftrightarrow H_nH_n^T=nI_n$(其中 H_n^T 表示 H_n 的转置方阵，I_n 表示 n 阶单位方阵)$\Longleftrightarrow H_n^TH_n=nI_n\Longleftrightarrow H_n$ 的任意两个不同的列正交.

(2) 法国数学家 Hadamard 一个著名的结果是说：若 M 是 n 阶实方阵(即元素均为实数)，如果每个元素的绝对值不超过1，则 M 的行列式的绝对值$\leqslant n^{\frac{n}{2}}$. 如果 H_n 是 n 阶阿达玛方阵，则 $H_nH_n^T=nI_n$. 两边取行列式知$(\det H_n)^2=n^n$. 于是 H_n 的行列式的绝对值等于 $n^{\frac{n}{2}}$. 即阿达玛阵是达到阿达玛上界 $n^{\frac{n}{2}}$的一批方阵.

(3) 阿达玛方阵在数字通信中有重要作用，用来作离散付立叶分析和快速计算.

例1 最简单的阿达玛阵是 $H_2=\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

由 H_2 可构作出4阶阿达玛阵

$$H_4=\begin{pmatrix}H_2 & H_2\\ H_2 & -H_2\end{pmatrix}=\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{bmatrix}$$

一般地，若 H_d 是 d 阶阿达玛阵，则不难证明

$$H_{2^d}=\begin{bmatrix}H_d & H_d\\ H_d & -H_d\end{bmatrix}$$

是 $2d$ 阶阿达玛阵. 于是对每个 $n\geqslant1$，均存在 2^n 阶阿达玛阵.

2.5.2 引理 设 $n\geqslant3$，如果存在 n 阶阿达玛阵，必然 $4\mid n$.

证明 设 $H_n=(a_{ij})$ 是 n 阶阿达玛阵. 由于 $n\geqslant3$，$a_{ij}=\pm1$，前三行彼此正交，因此

$$\begin{aligned}&\sum_{i=1}^{n}(a_{1j}+a_{2j})(a_{1j}+a_{3j})\\ &=\sum_{j=1}^{n}(a_{1j}^2+a_{1j}a_{3j}+a_{1j}a_{2j}+a_{2j}a_{3j})\\ &=\sum_{j=1}^{n}a_{1j}^2=n.\end{aligned}$$

但是 $a_{1j}+a_{2j}$ 和 $a_{1j}+a_{3j}$ 均为偶数. 所以上式左边可被4除尽. 因此 $4\mid n$. 证毕.

关于阿达玛阵的一个著名猜想是：

对于每个 $n\equiv0\pmod 4$，均存在 n 阶阿达玛阵.

目前已构作出许多阿达玛阵. 但是上述猜想至今未完全解决.

现在我们用有限域来构作阿达玛阵.

2.5.3 定义 设 q 为素数幂，$2\nmid q$. F_q^* 中元素 α 叫作平方元素，是指存在 $\beta\in F_q^*$，使得 $\alpha=\beta^2$. 否则，α 叫作 F_q^* 的非平方元素. 当 q 为奇素数 p 时，F_p^* 中的平方元素和非平方元素就是初等数论中所说的模 p 二次剩余和二次非剩余.

设 γ 是 F_q 的一个本原元素，则 F_q^* 中元素为 $\gamma^i(0\leqslant i\leqslant q-2)$. $\gamma^{q-1}=1$. 由于 $q-1$为偶数，易知：

$$\alpha=\gamma^i \text{ 为 } F_q^* \text{ 中平方元素} \iff i \text{ 为偶数} \qquad (*)$$

于是 F_q^* 中共有$\frac{q-1}{2}$个平方元素，它们是：$1,\gamma^2,\gamma^4,\gamma^6,\cdots,\gamma^{q-3}$. 而非平方元素也有$\frac{q-1}{2}$个，它们是：$\gamma,\gamma^3,\cdots,\gamma^{q-2}$.

对每个 $\alpha\in F_q^*$，定义函数

$$f(\alpha)=\begin{cases}1, & \text{若 } \alpha \text{ 为 } F_q^* \text{ 中平方元素.}\\ -1 & \text{若 } \alpha \text{ 为 } F_q^* \text{ 中非平方元素.}\end{cases}$$

再规定 $f(0)=0$. 下面是函数 f 的一些性质.

2.5.4 引理 设 q 为奇素数的方幂.

(1) 对 $a,b\in F_q$，$f(a)f(b)=f(ab)$.

(2) $\sum\limits_{a\in F_q}f(a)=\sum\limits_{a\in F_q^*}f(a)=0$.

(3) 设 $q\equiv 3 \pmod 4$，$a\in F_q^*$，则

$$\sum_{c\in F_q}f(c^2-a^2)=-1.$$

证明 (1) 当 a 或 b 等于0时，$0=f(a)f(b)=f(ab)=f(0)=0$. 若 $a,b\in F_q^*$，由(*)易知：两个平方元素之积或两个非平方元素之积均是平方元素，而平方元素和非平方元素之积是非平方元素. 再由 f 的定义即知 $f(ab)=f(a)f(b)$.

(2) 这是由于 $f(0)=0$，并且 F_q^* 中有一半是平方元素，另

一半是非平方元素.因此(2)的和式中有同样多个1和-1,相加为0.

(3) 由于 $a\neq 0$,从而

$$\sum_{c\in F_q} f(c^2-a^2)=\sum_{b\in F_q} f(a^2b^2-a^2) \qquad (令\ c=ab)$$

$$=f(a)^2\sum_{b\in F_q} f(b^2-1) \qquad (由(1))$$

$$=\sum_{b\in F_q} f(b^2-1)=f(-1)+\sum_{b\in F_q^*} f(b^2-1)$$

$$=-1+\sum_{b\in F_q^*} f(b^2-1). \left(\begin{array}{l}由于-1=\gamma^{\frac{q-1}{2}},而\dfrac{q-1}{2}为奇数,\\ 从而\ f(-1)=-1\end{array}\right)$$

但是 $$\sum_{b\in F_q^*} f(b^2-1)=\sum_{d\in F_q^*} f(d^{-2}-1)=\sum_{d\in F_q^*} f(1-d^2)\cdot f(d^{-2})$$

$$=\sum_{d\in F_q^*} f(1-d^2)=\sum_{d\in F_q^*} f(d^2-1)f(-1)$$

$$=-\sum_{d\in F_q^*} f(d^2-1)=-\sum_{b\in F_q^*} f(b^2-1).$$

于是$\sum_{b\in F_q^*} f(b^2-1)=0$.这就表明$\sum_{c\in F_q} f(c^2-a^2)=-1$.

2.5.5 定理 设 $F_q=\{a_1,a_2,\cdots,a_q\}$,$q\equiv 3 \pmod 4$.

则 $$H_{q+1}=\begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & -1 & b_{12} & b_{13} & \cdots & b_{1q} \\ 1 & b_{21} & -1 & b_{23} & \cdots & b_{2q} \\ & & \cdots\cdots\cdots & & & \\ 1 & b_{q1} & b_{q2} & b_{q3} & \cdots & -1 \end{bmatrix}$$

是 $q+1$阶阿达玛阵.其中 $b_{ij}=f(a_j-a_i)$.

证明 对于$1\leqslant i\leqslant q$,第1行和第 $i+1$行的内积为

$$1-1+\sum_{\substack{j=1,\\ j\neq i}}^{q} b_{ij}=\sum_{\substack{j=1\\ j\neq i}}^{q} f(a_j-a_i)=\sum_{a\in F_q^*} f(a)=0.$$

(因为当 $j=1,2,\cdots,q$ 时，a_j-a_i 过 F_q 中所有元素，而 $j=i$ 时 $a_j-a_i=0$). 当$1\leqslant i<\leqslant q+1$时，第$(i+1)$行和第$(k+1)$行的内积为

$$1-b_{ki}-b_{ik}+\sum_{j\neq i,k} b_{ij}b_{kj}$$

$$=1-f(a_i-a_k)-f(a_k-a_i)+\sum_{j\neq i,k} f(a_j-a_i)f(a_j-a_k).$$

由于 $f(-a)=f(-1)f(a)=-f(a)$，因此上式右边为

$$1+\sum_{c\in F_q} f(c^2-(a_i+a_k)c+a_ia_k)$$

$$=1+\sum_{c\in F_q} f\left(\left(c-\frac{a_i+a_k}{2}\right)^2-\left(\frac{a_i-a_k}{2}\right)^2\right)$$

（注意：由于 F_q 的特征是奇素数，2为 F_q 中非零元素）

$$=1+\sum_{c\in F_p} f(c^2-a^2),$$

其中 $a=\frac{a_i-a_k}{2}\neq 0$. 由引理2.5.4的(3)可知

$$1+\sum_{c\in F_q} f(c^2-a^2)=1-1=0.$$

这就表明方阵 H_{q+1}的任意两个不同的行都是正交的. 从而为阿达玛阵. 证毕.

利用引理2.5.4还可以构作差集合.

2.5.6 定理 设 p 为素数，$p\equiv 3 \pmod 4$. $d_1,\cdots,d_k$ 是模 p 的全体二次非剩余，则 $D=\{d_1,\cdots,d_k\}$ 是参数为 $(v,k,\lambda)=\left(p,\frac{p-1}{2},\frac{p-3}{4}\right)$ 的差集合.

证明 对每个 $a\in F_p^*$，易知当 $x\neq 0,-a$ 时，

$$(f(x)-1)(f(x+a)-1)=\begin{cases}4, & \text{若 } x \text{ 和 } x+a \text{ 均为二次非剩余} \\ 0, & \text{否则}\end{cases}$$

但是 x 和 $x+a$ 均为二次非剩余 $\Longleftrightarrow x, x+a \in D$

$\Longleftrightarrow D$ 中元素 $x+a$ 和 x 的差为 a.

因此集合 D 中相差为 a 的元素对的个数为

$$\lambda(a)=\frac{1}{4}\sum_{x\in F_p, x\neq 0,-a}(f(x)-1)(f(x+a)-1)$$

$$=\frac{1}{4}\sum_{x\in F_p, x\neq 0,-a}[f(x^2+ax)-f(x)-f(x+a)+1]$$

$$=\frac{1}{4}\left[\begin{array}{l}\sum_{x\in F_p}f(x^2+ax)-(\sum_{x\in F_p}f(x)-f(-a)) \\ \qquad -(\sum_{x\in F_p}f(x+a)-f(a))+p-2\end{array}\right]$$

$$=\frac{1}{4}\left[\sum_{x\in F_p}f\left((x+\frac{a}{2})^2-(\frac{a}{2})^2\right)+f(-a)+f(a)+p-2\right]$$

$$\left(\text{因为}\sum_{x\in F_p}f(x)=0\right)$$

$$=\frac{1}{4}\left[\sum_{x\in F_p}f\left(x^2-\left(\frac{a}{2}\right)^2\right)+p-2\right] \quad (\text{因为 } f(-a)=-f(a))$$

$$=\frac{1}{4}(p-3) \qquad (\text{由引理2.5.4的(3)}).$$

于是 $\lambda(a)=\frac{1}{4}(p-3)$ 是与 a 无关的常数. 根据定义即知 D 为参数 $(v,k,\lambda)=\left(p,\frac{p-1}{2},\frac{p-3}{4}\right)$ 的差集合.

例2 在定理2.5.6中取 $p=11$. 由于模11的二次剩余为1, $2^2=4, 3^2=9, 4^2=16=5$ 和 $5^2=25=3$, 从而二次非剩余构成的 $D=\{2,6,7,8,10\}$ 是参数 $(v,k,\lambda)=(11,5,2)$ 的差集合.

下面定理可由已知阿达玛阵构作新的阿达玛阵.

2.5.7 定理 如果存在 n 阶和 m 阶的阿达玛阵，则也存在 nm 阶的阿达玛阵.

证明 设 $H_n=(a_{ij})(1\leqslant i,j\leqslant n)$ 和 $H_m=(a_{kl})(1\leqslant k,l\leqslant m)$ 分别是 n 阶和 m 阶阿达玛阵. 对于 $a=\pm1$，我们以 aH_m 表示将 H_m 中每个元素乘以 a 而得到的 m 阶方阵. 请大家验证，nm 阶方阵

$$\begin{bmatrix} a_{11}H_m & a_{12}H_m & \cdots & a_{1n}H_m \\ a_{21}H_m & a_{22}H_m & \cdots & a_{2n}H_m \\ \cdots\cdots & & & \\ a_{n1}H_m & a_{n2}H_m & \cdots & a_{nn}H_m \end{bmatrix}$$

是阿达玛阵.

最后我们谈阿达玛阵和对称 BIBD 的关系.

2.5.8 定理 设 $n=4t$. 则：存在 n 阶阿达玛阵的充要条件是存在参数 $(v,k,\lambda)=(4t-1,2t-1,t-1)$ 的 BIBD.

证明 设 $H_n=(a_{ij})$ 是一个 n 阶阿达玛阵. 将 H_n 的某一行或其一列变号之后，仍是阿达玛阵. 所以我们不妨设 H_n 的第一行和第一列的所有元素全是1. 令 $X=\{2,3,\cdots,n\}$ 为品种集合，X 中以下 $n-1$ 个子集作为区组

$$X_i=\{j\,|\,2\leqslant j\leqslant n,a_{ij}=1\}\qquad(2\leqslant i\leqslant n).$$

我们证明 $\{X_2,X_3,\cdots,X_n\}$ 是参数 $(v,k,\lambda)=(4t-1,2t-1,t-1)$ 的对称 BIBD. 首先，当 i 或 j 为1时，$a_{ij}=1$. 由于第一行与第 i 行正交 $(2\leqslant i\leqslant n)$. 从而

$$0=\sum_{j=1}^{n}a_{1j}a_{ij}=1+\sum_{j=2}^{n}a_{ij}.$$

于是 $\sum_{j=2}^{n}a_{ij}=-1$. 另一方面，设 $a_{ij}(2\leqslant j\leqslant n)$ 当中有 k 个为1，则

另外 $n-k-1$ 个为 -1. 于是 $\sum_{j=2}^{n} a_{ij}=k-(n-k-1)=2k-n+1$. 于是 $-1=2k-n+1$, $k=\frac{n}{2}-1=2t-1$. 这就表明每个区组 X_i($2\leqslant i\leqslant n$)都有 $k=2t-1$ 个品种. 类似地,利用第一列和第 j 列正交($2\leqslant j\leqslant m$),可证得每个品种均恰好在 k 个区组之中. 最后设 i 和 j 是两个不同的品种,即 $2\leqslant i\neq j\leqslant n$. 则:

i 和 j 同时在区组 X_h 中 $\Longleftrightarrow a_{hi}=a_{hj}=1$. 设 i 和 j 同时出现在 λ 个区组 X_h($2\leqslant h\leqslant n$)之中. 即有 λ 个 h 值使得 $a_{hi}=a_{hj}=1$. 由于 a_{hi}($2\leqslant h\leqslant n$)中共有 $k=2t-1$ 个为1,从而对于剩下的 $k-\lambda$ 个 h 值, $a_{hi}=1$, $a_{hj}=-1$. 同样地也有 $k-\lambda$ 个 h 值,使 $a_{hi}=-1$, $a_{hj}=1$. 最后剩下 $n-1-2(k-\lambda)-\lambda$ 个 h 值,使 $a_{hi}=a_{hj}=-1$. 于是由第 i 列和第 j 列正交,可知

$$\begin{aligned}-1=\sum_{h=2}^{n} a_{hi}a_{hj}&=\lambda-2(k-\lambda)+n-1-2(k-\lambda)-\lambda\\&=n-1-4(k-\lambda).\end{aligned}$$

从而 $\lambda=k-\frac{n}{4}=2t-1-t=t-1$. 即任意两个不同品种均恰好同时出现在 $t-1$ 个区组之中. 于是 $\{X_2,X_3,\cdots,X_n\}$ 是参数 $(v,k,\lambda)=(4t-1,2t-1,t-1)$ 的对称 BIBD.

反过来,设 $X=\{2,3,\cdots,n\}$ 为品种, $\{X_2,\cdots,X_n\}$ 为 X 的 $n-1$ 个子集,并且以 $X_2,\cdots,X_n$ 为区组构成参数 $(v,k,\lambda)=(4t-1,2t-1,t-1)$ 的对称 BIBD($n=4t$). 对于 $2\leqslant i,j\leqslant n$,令

$$a_{ij}=\begin{cases}1, & 若\ j\in X_i\\ -1, & 若\ j\notin X_i.\end{cases}$$

再令 $a_{11}=a_{12}=\cdots=a_{1n}=a_{21}=a_{31}=\cdots=a_{n1}=1$. 将上面的证明反其道而行之,可证 $H_n=(a_{ij})$($1\leqslant i,j\leqslant n$)是 n 阶阿达玛阵.

2.5.9 习　题

1. 试构造12阶阿达玛阵.
2. 试构作参数$(v,k,\lambda)=(19,9,4)$和$(23,11,5)$的差集合.

§2.6　q元序列

考虑下面的序列

$$a_0a_1a_2\cdots=122021100\ 122021100\ 122021100\ \cdots\cdots$$

序列中每个数字是0,1或2.这是周期为9的序列,即$a_n=a_{n+9}$ $(n=0,1,2,\cdots)$.序列中任意9个连续数字如(从头开始)122021100或者(从a_2开始)202110012等都叫作此序列的一个周期节而序列中任意连续两位都叫它的一个状态.周期为9的序列最多有9个不同状态(因为$a_na_{n+1}=a_{n+9}a_{n+10}$),而此序列前9个状态均不相同:12,22,20,02,21,11,10,00,01.所以恰好是由{0,1,2}组成的所有可能的状态.

再考虑序列

$$a_0a_1a_2\cdots=01011001000011110101100100001111\cdots\cdots$$

这是周期为16的序列,每位数字是0或1.现在把其中任意连续四位叫作一个状态,则此序列中出现的16个状态:0101,1011,0110,1100,…,1111,1110,1101,1010 恰好是由{0,1}组成的所有可能的状态!

2.6.1　定义　设S是k元集合,$0\in S$.一个**k元序列**是指

$$\underline{a} = a_0a_1a_2\cdots\cdots \qquad a_i \in S.$$

通常这个序列是无限的. 而有限序列 $a_0a_1a_2\cdots a_n$ 则等同于无限序列 $a_0a_1a_2\cdots a_n00\cdots$.

k 元序列$\underline{a}$叫作周期序列,是指存在正整数 N,使得

$$a_n = a_{n+N} \qquad (n = 0,1,2,\cdots), \tag{1}$$

而满足此条件的最小正整数叫作序列$\underline{a}$的周期,表示成 $p(\underline{a})$. 由除法算式可知,正整数 N 满足(1)的充要条件是 $p(\underline{a})|N$. 所以每个满足(1)的 N 也叫作周期倍数. 对于每个 n, $a_na_{n+1}\cdots a_{n+p(\underline{a})-1}$(即序列中任意连续 $p(\underline{a})$位数字)都叫序列$\underline{a}$的一个周期节.

如果$\underline{a}$是周期为 $k^n(n\geqslant1)$的 k 元序列,并且$\underline{a}$中前 k^n 个长为 n 的状态:

$$a_0a_1\cdots a_{n-1}, a_1a_2\cdots a_n, a_2a_3\cdots a_{n+1}, \cdots,$$

$$a_{k^n-1}a_{k^n}a_{k^n+1}\cdots a_{k^n+n-2} = a_{k^n-1}a_0a_1\cdots a_{n-2}$$

两两不同,从而恰好是由 S 中 k 个元素构成的所有 k^n 个状态. 则$\underline{a}$叫作 n级 k元 M序列.

本节开头的两个例子,分别是2级3元 M 序列和4级2元 M 序列.

M 序列一开始也是以数学游戏的形式出现的. 近年来,它被用于保密通讯中,作为加密的一种工具和手段. 原因是这个序列有所谓"伪随机性",从而利用它可以把原始信息有效地掩盖起来. 另一方面,M 序列的数目惊人地多,敌方很难知道用的是哪一个,所以不易破密.

对于周期序列$\underline{a}=a_0a_1\cdots$,令 $L\,\underline{a}=a_1a_2\cdots\cdots$,序列 $L\,\underline{a}$叫作$\underline{a}$的左平移序列. 更一般地,对每个 $k\geqslant0$,令 $L^k\,\underline{a}=a_ka_{k+1}\cdots$. 若$\underline{a}$和$\underline{b}$均是周期为 P 的序列. 如果 $L^k\,\underline{a}=\underline{b}$, $0\leqslant k\leqslant P-1$,易知 $L^{P-k}\underline{b}=$

a. 这时，我们称a和b是平移等价的. 今后我们把彼此平移等价的周期序列看成是同一个序列. 可以证明：n 级 k 元 M 序列的个数是

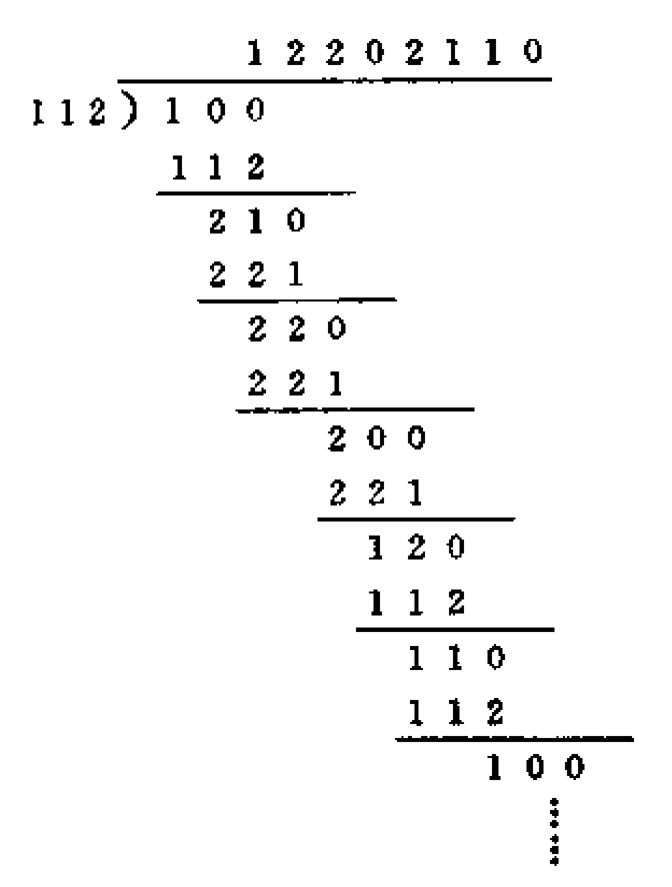
$$((k-1)!)^{k^{n-1}}k^{k^{n-1}-n},$$

这个数目的计算是采用图论方法，由于本质上没有用到有限域的知识，此处从略. 但由此可见，M 序列的数目是很多的. 由于它在通信技术中的用处，一个自然的问题是：这些 M 序列如何具体构作出来？我们又可以利用有限域，随手便可得到 M 序列的例子.

我们用 $F_3[x]$中的多项式$1+x+2x^2$以升幂的方式去除1，则有如下的算式：

$$
\begin{array}{l}
\qquad\qquad\qquad 1+2x+2x^2+0+2x^4+x^5+x^6+0+x^8+\cdots \\
1+x+2x^2\,)\,\overline{1+0+0} \\
\qquad\qquad\quad \underline{1+x+2x^2} \\
\qquad\qquad\qquad 2x+x^2+0 \\
\qquad\qquad\qquad \underline{2x+2x^2+x^3} \\
\qquad\qquad\qquad\quad 2x^2+2x^3+0 \\
\qquad\qquad\qquad\quad \underline{2x^2+2x^3+x^4} \\
\qquad\qquad\qquad\qquad 2x^4+0+0 \\
\qquad\qquad\qquad\qquad \underline{2x^4+2x^5+x^6} \\
\qquad\qquad\qquad\qquad\quad x^5+2x^6+0 \\
\qquad\qquad\qquad\qquad\quad \underline{x^5+x^6+2x^7} \\
\qquad\qquad\qquad\qquad\qquad x^6+x^7+0 \\
\qquad\qquad\qquad\qquad\qquad \underline{x^6+x^7+2x^8} \\
\qquad\qquad\qquad\qquad\qquad\quad x^8+0+0 \\
\qquad\qquad\qquad\qquad\qquad\qquad \vdots
\end{array}
$$

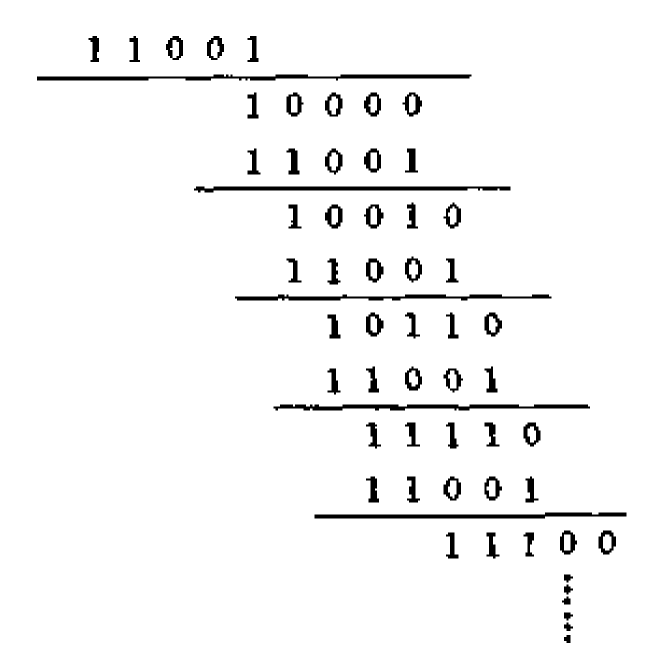
为简单起见，去掉 $x^i(i=1,2,\cdots)$而只保留它们的系数，则上面的算式可缩写成（如$1+x+2x^2$缩写为112）：



读者看到，最后的余式100与开头已经一样了，所以商式接下来又是12202110……. 所以整个商式便应当为以12202110为开头周期节、周期为7的三元序列. 将此周期节增加一个0而为122021100…，就成了本节开头第一个例子.

我们再用 $F_2[x]$中的多项式$1+x+x^4$（缩写成11001）去除多项式 $x+x^2+x^3$（缩写成0111），用升幂方式相除则为

```
          0 1 0 1 1 0 0 1 0 0 0 1 1 1 1
11001 ) 0 1 1 1 0 0
          1 1 0 0 1
          ---------
            1 0 1 0 0
            1 1 0 0 1
            ---------
              1 1 0 1 0
              1 1 0 0 1
              ---------
                  1 1 0 0 0
```



于是得到周期15的二元序列. 将开头周期节010110010001111的连续有三个0的地方再塞进一个0之后,变成周期16的二元序列,就是本节开头的第二个例子.

设 $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$ 为 $F_q[x]$中多项式,$a_0a_n\neq 0$. 我们把多项式

$$\hat{f}(x)=x^nf\left(\frac{1}{x}\right)=a_0+a_1x+\cdots+a_nx^n$$

叫作 $f(x)$的**反向多项式**. 不难看出:(1) α 为 $f(x)$的根$\Longleftrightarrow\alpha^{-1}$为 $\hat{f}(x)$的根(注意:由于 $a_0a_n\neq 0$,从而0不为 $f(x)$和 $\hat{f}(x)$的根). (2) $f(x)$不可约$\Longleftrightarrow\hat{f}(x)$不可约.

也许读者注意到,我们刚才作除法时使用的 $F_3[x]$中多项式$1+x+2x^2$是本原多项式 x^2+x+2的反向多项式,而 $F_3[x]$中的$1+x+x^4$也是本原多项式 x^4+x^3+1的反向多项式. 对于任意有限域 F_q 和 $F_q[x]$中任意 n 次本原多项式 $f(x)$. 用 $f(x)$以升幂方式去除 $F_q[x]$中任意次数$<n$ 的多项式 $g(x)$,得到的商必然是周期 q^n-1的 q 元序列. 在此序列的周期节有连续 $n-1$个0的地方再塞进一个0,得到的周期 q^n 的序列一定是 n 级 q 元 M

序列!读者若不相信,可以自行验证.

现在我们就来解释其中的奥妙.也就是要讲述如何用有限域构作 M 序列.为了把事情看的更清楚,我们需要使用一个新的代数结构——有限域上的幂级数环.

如上所述,我们把元素属于 $\boldsymbol{F}_q$ 的一个 q 元序列

$$\underline{a} = a_0a_1a_2\cdots a_n\cdots\cdots \qquad (a_i \in \boldsymbol{F}_q)$$

看成是一个无限的"多项式"

$$A(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n+\cdots$$

这种无限的多项式在数学上叫作**幂级数**.通常的多项式 $a_0+a_1x+\cdots+a_nx^n$ 看成 $a_0+a_1x+\cdots+a_nx^n+0\cdot x^{n+1}+0\cdot x^{n+2}+\cdots$,从而有限序列 $a_0a_1a_2\cdots a_n$ 看成是 $a_0a_1\cdots a_n00\cdots\cdots$.两个幂级数

$$A(x)=a_0+a_1x+\cdots=\sum_{n=0}^{\infty}a_nx^n,B(x)=b_0+b_1x+\cdots=\sum_{n=0}^{\infty}b_nx^n \tag{2}$$

相等,当且仅当对应系数均相等,即 $a_n=b_n(n=0,1,\cdots)$.所有这种幂级数组成的集合表示成 $\boldsymbol{F}_q[[x]]$.由于每个多项式均看成幂级数,所以多项式集合 $\boldsymbol{F}_q[x]$看成是 $\boldsymbol{F}_q[[x]]$的子集.

但是多项式集合 $\boldsymbol{F}_q[x]$中是有加法和乘法的.并且 $\boldsymbol{F}_q[x]$对于这些运算形成环,即满足定义1.2.1中除了(Ⅰ.4)以外的所有公理.现在也可仿照多项式的运算来定义幂级数的运算.对于(2)式中的幂级数 $A(x)$和 $B(x)$,定义自然的加法

$$A(x)+B(x)=(a_0+b_0)+(a_1+b_1)x+(a_2+b_2)x^2+\cdots$$

$$=\sum_{n=0}^{\infty}(a_n+b_n)x^n.$$

对于乘法,也与多项式乘法类似(即先用分配律,然后再合并同类项):

$$A(x)B(x)=a_0b_0+(a_0b_1+a_1b_0)x+(a_0b_2+a_1b_1+a_2b_0)x^2+\cdots$$

$$=c_0+c_1x+c_2x^2+\cdots+c_nx^n+\cdots$$

其中

$$c_n=\sum_{i=0}^{n}a_ib_{n-i}.$$

可以象多项式的情形一样验证：幂级数集合 $\boldsymbol{F}_q[[x]]$对于如此定义的加法和乘法形成一个(交换)环，即定义1.2.1中除了(Ⅰ.4)之外其余公理均成立. 于是 $\boldsymbol{F}_q[[x]]$叫作 $\boldsymbol{F}_q$ 上的**幂级数环**，而多项式环 $\boldsymbol{F}_q[x]$是它的一个子环. $\boldsymbol{F}_q[[x]]$中的减法自然为

$$A(x)-B(x)=\sum_{n=0}^{\infty}(a_n-b_n)x^n.$$

$\boldsymbol{F}_q[x]$和 $\boldsymbol{F}_q[[x]]$均不是域，定义1.2.1中的公理(Ⅰ.4)不成立. 也就是说，不是每个非零元素均可逆. 在一个环中可逆元素愈多，作除法的自由性就愈大，这个环就愈接近于域. 在多项式环 $\boldsymbol{F}_q[x]$中，多项式 $f(x)$可逆的充要条件是 $f(x)$实际上为 $\boldsymbol{F}_q$ 中非零元素. 因为当 $f(x)$的次数$\geqslant 1$时，有理函数$1/f(x)$不是多项式，即 $f(x)$在 $\boldsymbol{F}_q[x]$中没有逆. 所以 $\boldsymbol{F}_q[x]$中的可逆元素是很少的. 有趣的是，当我们允许多项式有无穷多项，即把$\boldsymbol{F}_q[x]$扩大成 $\boldsymbol{F}_q[[x]]$之后，$\boldsymbol{F}_q[[x]]$中有相当多的可逆元素(见下面引理). 从这个意义上讲，幂级数环 $\boldsymbol{F}_q[[x]]$比多项式环 $\boldsymbol{F}_q[x]$要好.

2.6.2 引理 $\boldsymbol{F}_q[[x]]$中元素

$$A(x)=a_0+a_1x+\cdots+a_nx^n+\cdots$$

可逆的充要条件是 $a_0\neq 0$(即 $a_0\in \boldsymbol{F}_q^*$).

证明 设 $A(x)$可逆，则有幂级数 $B(x)=b_0+b_1x+\cdots$ 使得

$$1=A(x)B(x)$$

$$=a_0b_0+(a_0b_1+a_1b_0)x+(a_0b_2+a_1b_1+a_2b_0)x^2+\cdots \quad (3)$$

于是 $a_0b_0=1$. 从而 $a_0\neq 0$. 反之若 $a_0\neq 0$，我们可待定 $B(x)$的所有系数 b_n 使得(3)式成立. 由(3)式知

$$1=a_0b_0,$$
$$0=a_0b_1+a_1b_0=a_0b_2+a_1b_1+a_2b_0=\cdots$$
$$=a_0b_n+a_1b_{n-1}+\cdots+a_nb_0=\cdots$$

从而可依次求出：

$$b_0=a_0^{-1},\quad b_1=-a_0^{-1}a_1b_0,\quad b_2=-a_0^{-1}(a_1b_1+a_2b_0),\cdots$$
$$b_n=-a_0^{-1}(a_1b_{n-1}+a_2b_{n-2}+\cdots+a_nb_0),\cdots$$

对于如此求出的 $b_n(n=0,1,2,\cdots)$，$B(x)=b_0+b_1x+b_2x^2+\cdots$显然为 $A(x)$的逆，即 $A(x)$是 $\boldsymbol{F}_q[[x]]$中可逆元素. 证毕.

于是在 $\boldsymbol{F}_q[[x]]$中我们便有许多可逆元. 下面例子虽然简单，但是很基本.

例1 $1-x^n$ 为 $\boldsymbol{F}_q[x]$中可逆元素. 容易看出

$$\frac{1}{1-x^n}=1+x^n+x^{2n}+x^{3n}+\cdots$$

而对于每个次数小于 n 的多项式 $a_0+a_1x+\cdots+a_{n-1}x^{n-1}$，

$$\frac{a_0+a_1x+\cdots+a_{n-1}x^{n-1}}{1-x^n}$$
$$=(a_0+a_1x+\cdots+a_{n-1}x^{n-1})(1+x^n+x^{2n}+\cdots)$$
$$=a_0+a_1x+\cdots+a_{n-1}x^{n-1}+a_0x^n+a_1x^{n+1}+\cdots+a_{n-1}x^{2n-1}+\cdots$$

它对应的 q 元序列 $a_0a_1\cdots a_{n-1}a_0a_1\cdots a_{n-1}\cdots$为周期序列，并且 n 是此序列的周期倍数(即周期为 n 或 n 的真因子).

对每个多项式 $f(x)\in\boldsymbol{F}_q[x]$，$f(0)\neq 0$(即 $f(x)$为$\boldsymbol{F}_q[[x]]$中可逆元素)，我们在第1.5节定义了 $f(x)$的周期，$p(f)$，即满足 $f(x)\mid x^n-1$的最小正整数 n. 读者从下面定理中可知为什么要采用“周期”这个名字.

2.6.3 定理 设$\underline{a}=a_0a_1\cdots a_n\cdots$是 q 元序列($a_i\in \boldsymbol{F}_q$),$A(x)=\sum_{n=0}^{\infty}a_nx^n$ 是对应的幂级数. 则

(1) $\underline{a}$为周期序列$\Longleftrightarrow A(x)$可表成真分式 $A(x)=\dfrac{g(x)}{f(x)}$,其中 $f(x),g(x)\in \boldsymbol{F}_q[x]$,$f(0)\neq 0$,$\deg g(x)<\deg f(x)$.

(2) 若 $A(x)=\dfrac{g(x)}{f(x)}$是既约的真分式,即 f 和 g 互素,则$\underline{a}$的周期等于 $f(x)$的周期,即 $p(\underline{a})=p(f)$.

(3) 若 $f(x)$为 $\boldsymbol{F}_q[x]$中不可约多项式,则对每个 $g(x)\in \boldsymbol{F}_q[x]$,$g(x)\neq 0$,$\deg g<\deg f$,$A(x)=\dfrac{g(x)}{f(x)}$对应的序列$\underline{a}$均是周期为 $p(f)$的 q 元序列. 如果 $\deg f=n$,则$\underline{a}$的周期为 q^n-1的因子. 并且$\underline{a}$的周期为 q^n-1的充要条件是 $c_n^{-1}f(x)$为 n 次本原多项式,这里 c_n 为 $f(x)$的首项系数.

证明 设序列$\underline{a}$的周期为 m,则

$$A(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}+a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x^{2n-1}+\cdots$$

$$x^nA(x)=a_0x^n+a_1x^{n+1}+\cdots+a_{n-1}x^{2n-1}+\cdots,$$

于是$(1-x^n)A(x)=A(x)-x^nA(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}$. 从而

$$A(x)=\frac{a_0+a_1x+\cdots+a_{n-1}x^{n-1}}{1-x^n}$$

为真分式,反之若 $A(x)=\dfrac{g(x)}{f(x)}$是真分式,并且 $f(0)\neq 0$. 令 $n=p(f)$是 f 的周期,则 $f(x)\,|\,1-x^n$. 于是有 $h(x)\in \boldsymbol{F}_q[x]$,使得 $fh=1-x^n$. 于是

$$A(x)=\frac{g(x)h(x)}{1-x^n}.$$

由 $\deg g < \deg f$ 可知 $\deg g(x)h(x) < \deg f(x)h(x) = \deg(1-x^n) = n$. 从而 $g(x)h(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$. 于是由例1即知 $A(x)$是周期序列. 并且周期为 $n = p(f)$的因子.

(2) 若 $A(x) = \frac{g(x)}{f(x)}$为既约真分式. 记 $n = p(\underline{a})$. 由(1)的证明知 $n \mid p(f)$. 另一方面，又有

$A(x) = \frac{h(x)}{1-x^n}$, $\deg h(x) < n$. 于是$\frac{g(x)}{f(x)} = \frac{h(x)}{1-x^n}$，从而 $f(x) \mid g(x)(1-x^n)$. 由于 f 和 g 互素，因此 $f(x) \mid 1-x^n$. 从而 $p(f) \mid n$. 所以 $p(f) = n = p(\underline{a})$.

(3) 我们知道：$F_q[x]$中 n 次不可约多项式的周期均为 q^n-1的因子，并且周期为 q^n-1的充要条件是 $C_n^{-1}f(x)$为本原多项式($f(x)$乘以 C_n^{-1} 只是为了作成首1多项式). 所以由(2)立刻推出(3).

例2 令 $q=2$, $1+x^2$, $1+x+x^3+x^5 \in F_2[x]$. $A(x) = \frac{1+x^2}{1+x+x^3+x^5}$. 由于分子分母的最大公因子为$1+x$，从而将 $A(x)$化成既约真分式$\frac{1+x}{1+x^3+x^4}$. 注意$1+x^3+x^4$是 $F_2[x]$中本原多项式. 所以 $A(x)$对应的二元序列$\underline{a}$周期为15.

注记 设 $A(x) = \frac{g(x)}{f(x)}$为真分式，$f(0) \neq 0$. 若 $f(0) = c_0$，则 $A(x) = \frac{c_0^{-1}g(x)}{c_0^{-1}f(x)}$，这时分母的常数项为1，由于 $c_0^{-1}f$ 和 f 的周期相同，所以今后我们总假定 $f(x)$的常数项为1，即 $f(0)=1$. 这时 $f(x) = 1 + c_1x + \cdots + c_nx^n$，而它的反向多项式为首1多项式 $\tilde{f}(x) = x^n + c_1x^{n-1} + \cdots + c_n$. 易知：$f(x)$不可约$\Longleftrightarrow \tilde{f}(x)$不可约. 并且定理2.6.3的(3)中所述条件 $c_n^{-1}f(x)$本原相当于说 $\tilde{f}(x)$本

原.

2.6.4 定理 设 $f(x),g(x)\in \boldsymbol{F}_q[x]$, $f(0)=1$, $\deg f=n>\deg g(x)$, $g(x)\neq 0$. $A(x)=\dfrac{g(x)}{f(x)}$对应于 q 元周期序列$\underline{a}=a_0a_1\cdots a_n\cdots$, $P=p(\underline{a})$. 我们把$\underline{a}$中每相邻 n 位 $a_ia_{i+1}\cdots a_{i+n-1}$叫作$\underline{a}$的一个**状态**. 则

(1) $\underline{a}$的前 P 个状态

$$a_ia_{i+1}\cdots a_{i+n-1} \qquad (i=0,1,\cdots,P-1)$$

是彼此不同的.

(2) 若 $f(x)$为 $\boldsymbol{F}_q[x]$中 n 次本原多项式. 将$\underline{a}$的一个周期节(首尾相接)中某个连续 $n-1$个0的地方再添加一个0,得到的周期为 q^n 的序列必为 n 级 q 元 M 序列.

证明 (1)设 $f(x)=1+c_1x+\cdots+c_nx^n$,

$$g(x)=b_0+b_1x+\cdots+b_{n-1}x^{n-1},$$

$$c_i,b_j\in \boldsymbol{F}_q, \qquad c_n\neq 0.$$

则
$$\begin{aligned}
&b_0+b_1x+\cdots+b_{n-1}x^{n-1}\\
&=g(x)=f(x)(a_0+a_1x+\cdots+a_nx^n+\cdots)\\
&=(1+c_1x+c_2x^2+\cdots+c_nx^n)(a_0+a_1x+\cdots+a_nx^n+\cdots)\\
&=a_0+(a_0c_1+a_1)x+(a_0c_2+a_1c_1+a_2)x^2+\cdots\\
&\quad+(a_0c_{n-1}+a_1c_{n-2}+\cdots+a_{n-2}c_1+a_{n-1})x^{n-1}\\
&\quad+(a_0c_n+a_1c_{n-1}+\cdots+a_{n-1}c_1+a_n)x^n+\cdots
\end{aligned}$$

由此得到
$$\begin{aligned}
&a_0=b_0,\\
&a_1=b_1-a_0c_1,\\
&a_2=b_2-(a_0c_2+a_1c_1), \qquad\qquad (4)\\
&\vdots\\
&a_{n-1}=b_{n-1}-(a_0c_{n-1}+a_1c_{n-2}+\cdots+a_{n-2}c_1).
\end{aligned}$$

而当 $i\geqslant0$时，

$$a_{n+i}=-(a_ic_n+a_{i+1}c_{n-1}+\cdots+a_{n+i-1}c_1).\qquad(5)$$

这表明当 $i\geqslant0$时，a_{n+i}由它前面的 n 个数字 $a_{n+i-1},a_{n+i-2},\cdots,a_{i+1},a_i$ 所决定，换句话说，由每个状态 $a_ia_{i+1}\cdots a_{n+i-1}$决定此状态后面的数字 a_{n+i}.

如果$\underline{a}$的前 P 个状态当中有两个相同，即有$0\leqslant i<j\leqslant P-1$，使得

$$a_ia_{i+1}\cdots a_{i+n-1}=a_ja_{j+1}\cdots a_{j+n-1}.$$

由(5)式可知 $a_{i+n}=a_{j+n}$. 于是 $a_{i+1}a_{i+2}\cdots a_{i+n}=a_{j+1}a_{j+2}\cdots a_{j+n}$. 由(5)式又有 $a_{i+n+1}=a_{j+n+1}$. 如此下去可知对每个 $l\geqslant0$均有 $a_{j+l}=a_{i+l}$，即

$$a_{j-i+k}=a_k\qquad(\text{当 } k\geqslant i \text{ 时}).\qquad(6)$$

由于$\underline{a}$是周期序列，可知(6)式对 $k=0,1,\cdots,i-1$也成立. 这表明 $j-i$ 是序列(6)的周期倍数. 于是 $P\mid j-i$, $0<j-i\leqslant P-1<P$, 这就导致矛盾. 从而$\underline{a}$的前 P 个状态彼此不同.

(2) 若 $f(x)$为 $F_q[x]$中本原多项式，则当 $g(x)\neq0$, $\deg g(x)<n$ 时，$A(x)=\dfrac{g(x)}{f(x)}$对应的序列$\underline{a}$具有周期 q^n-1(即 $f(x)$的周期). 从而$\underline{a}$的前 q^n-1个状态

$$a_ia_{i+1}\cdots a_{i+n-1}\qquad(0\leqslant i\leqslant q^n-2)$$

彼此不同. 但是这个序列$\underline{a}$中不会有全0状态$00\cdots0$(n 个0)(因否则由(5)式知$\underline{a}$必为全零序列，于是 $g(x)=0$.)于是$\underline{a}$的前 q^n-1 个状态就是由 q 个元素作成的所有可能非零状态. 如果按(2)中所述办法再加上一个0(注意$\underline{a}$中必有状态$0\cdots0b$($b\in F_q^*$)，从而周期节中共有 $q-1$个地方有连续 $n-1$个0)，则周期节中有 q^n 个元素，而前 q^n 个状态恰好为由 F_q 中 q 个元素组成的所有可能状态. 于是得到了 n 级 q 元 M 序列. 证毕.

到此为止我们完全解开了本节开始时所说的奥妙，即用$F_q[x]$中一个n次本原多项式的反向多项式以升幂方法去除任意一个次数小的非零多项式，所得序列在适当地方加入一个0之后，便得到一个n级q元M序列.

2.6.5 定义 设$f(x)=1+c_1x+\cdots+c_nx^n\in F_q[x]$，$c_n\neq0$. 则满足(5)式的$q$元周期序列叫作$n$级线性递归序列. 而$f(x)$叫作此线性递归序列的生成多项式.

今后，用$S(f)$表示以$f(x)$为生成多项式的所有周期序列组成的集合. 这些序列一一对应于真分式$\frac{g(x)}{f(x)}=A(x)$，其中$g(x)$的次数小于$f(x)$的次数n. 从而共有q^n个$g(x)$. 于是$S(f)$中共有q^n个序列($n=\deg f$). 给了$g(x)$之后，用升幂除法可得到$\underline{a}$，即$a_0,a_1,\cdots,a_n,\cdots$由(4)和(5)式求出. 反之，给了$S(f)$中的序列$\underline{a}=a_0a_1\cdots$，那末$g(x)=b_0+b_1x+\cdots+b_{n-1}x^{n-1}$的诸系数可以用$\underline{a}$的前$n$位求出，因为由(4)式我们有

$$
\begin{aligned}
&b_0=a_0,\\
&b_1=a_0c_1+a_1,\\
&b_2=a_0c_2+a_1c_1+a_2,\\
&\vdots\\
&b_{n-1}=a_0c_{n-1}+a_1c_{n-2}+\cdots+a_{n-2}c_1+a_{n-1}.
\end{aligned}
$$

但是，$S(f)$中q^n个序列可能有一些是彼此平移等价的. 如果$\underline{a}=a_0a_1\cdots$为$S(f)$中序列，那末，它的左平移序列$L\,\underline{a}=a_1a_2\cdots$是否也属于$S(f)$?下面定理给出肯定的答案.

2.6.6 定理 设$f(x)\in F_q[x]$，$\deg f=n$，$f(0)=1$. $\underline{a}$是$S(f)$中序列(周期为P)，对应幂级数为$\frac{g(x)}{f(x)}$. 对每个N，$0\leqslant N$

$\leqslant P-1$，若以$[x^{P-N}g(x)]$表示除法算式

$$x^{P-N}g(x)=q(x)f(x)+r(x),\quad \deg r(x)<n=\deg f(x),$$

得到的余式 $r(x)$，则 $L^N\underline{a}=a_Na_{N+1}\cdots$对应的幂级数为 $[x^{P-N}g(x)]/f(x)$. 从而 $L^N\underline{a}$也属于 $S(f)$.

证明 设

$$[x^{P-N}g(x)]/f(x)=b_0+b_1x+b_2x^2+\cdots \tag{7}$$

这是 $S(f)$中周期序列，由于

$$\begin{aligned}&[x^{P-N}g(x)]/f(x)\\&=\frac{x^{P-N}g(x)-q(x)f(x)}{f(x)}=x^{P-N}\frac{g(x)}{f(x)}-q(x)\\&=x^{P-N}(a_0+a_1x+\cdots+a_nx^n+\cdots)-q(x).\end{aligned}$$

因为 $q(x)$为 $F_q[x]$中多项式，由(7)式知当 $n>\deg q(x)$时，$a_n=b_{P-N+n}$，即对充分大的 n，$b_n=a_{n+N-P}=a_{b+N}$. 由于 $b_0b_1\cdots$和 $a_0a_1\cdots$都是周期序列，所以对每个 $n\geqslant 0$，均有 $b_n=a_{n+N}$. 于是 $b_0b_1\cdots=a_Na_{N+1}\cdots=L^N\underline{a}$. 这就证明了定理2.6.6.

由上述定理可知，$S(f)$中每个周期序列的平移序列仍属于 $S(f)$. 所以 $S(f)$中 q^n 个周期序列分成许多平移等价类. 如果象过去那样，我们把彼此平移等价的序列看作是同一个序列. 于是自然提出下面一个基本问题：

对于给定的 n 次多项式 $f(x)\in F_q[x]$，$f(0)=1$，$S(f)$中2^n个序列共分成多少平移等价类?每个等价类的周期是多少?

首先，对于每个 $f(x)$，$S(f)$中必有全零序列(对应$0/f(x)$)，它的周期为1. 其次，若 $f(x)$为 $F_q[x]$ 中 n 次不可约多项式，设 $P=p(f)$为 f 的周期，则 P 为 q^n-1的因子. 并且由定理2.6.3知道，$S(f)$中每个非零序列的周期均为 P. 从而每 P 个序列形成一个平移等价类，于是 $S(f)$中非零序列共有$\frac{q^n-1}{P}$个平移等价类，它们的周期均为 P. 特别当 $f(x)$是 n 次本原多项

式时，$P=q^n-1$. 于是 $S(f)$ 中非零序列只有一个（周期为 q^n-1），即 $S(f)$ 中任意两个非零序列均平移等价.

对于一般的 $f(x)$，为了弄清 $S(f)$ 的周期特性，我们引进如下符号：

2.6.7 定义 用 $\{P\}$ 表示周期为 P 的一个序列的平移等价类，它是由 P 个序列构成的等价类. 对每个 $f(x)\in \boldsymbol{F}_q[x]$，$f(0)=1$，$\deg f=n$，如果 $S(f)$ 中 q^n 个序列的周期分别为 $P_1,\cdots,P_s$，并且周期为 P_i 的序列共有 m_i 个平移等价类（$1\leqslant i\leqslant s$），我们称 $S(f)$ 的**周期结构**为

$$Z(f)=m_1\{P_1\}+\cdots+m_s\{P_s\}.$$

显然 $m_1P_1+\cdots+m_sP_s=q^n$.

我们以 R 表示形如 $m_1\{P_1\}+\cdots+m_r\{P_r\}$ 的所有元素构成的集合，其中 $m_i\in\boldsymbol{Z}$，P_i 为正整数（$1\leqslant i\leqslant r$）. 并且在集合 R 中引入加法和乘法. 加法为

$$\sum_{i=1}^{r}m_i\{P_i\}+\sum_{i=1}^{r}m_i'\{P_i\}=\sum_{i=1}^{r}(m_i+m_i')\{P_i\}.$$

而乘法定义为（用 $\odot$ 表示乘法）：

$$\{P_1\}\odot\{P_2\}=(P_1,P_2)\{[P_1,P_2]\}.$$

其中 (P_1,P_2)，$[P_1,P_2]$ 分别表示 P_1 和 P_2 的最大公因子和最小公倍数. 然后用分配律定义 R 中任意两个元素的乘积为

$$\begin{aligned}\Big(\sum_{i=1}^{r}m_i\{P_i\}\Big)\odot\Big(\sum_{j=1}^{s}n_j\{Q_j\}\Big)&=\sum_{i=1}^{r}\sum_{j=1}^{s}m_in_j\{P_i\}\odot\{Q_j\}\\&=\sum_{i=1}^{r}\sum_{j=1}^{s}m_in_j(P_i,Q_j)\{[P_i,Q_j]\}.\end{aligned}$$

不难验证，R 对于如上定义的加法和乘法形成（交换）环，即满足

定义1.2.1中除了(Ⅰ.4)以外的所有公理.这个环中的零元素为0,幺元素为$\{1\}$.

下面定理完全解决了$S(f)$的周期结构问题.

2.6.8 定理 设$f(x)$为$\mathbf{F}_q[x]$中n次多项式,$f(0)=1$.

(1) 如果$f(x)=g(x)^b$,其中$g(x)$为$\mathbf{F}_q[x]$中m次不可约多项式(于是$n=mb$),$b\geqslant 1$,$g(x)$的周期为e.设q为素数p的幂,令λ是满足$p^\lambda\leqslant b$的最大整数.则$S(f)$的周期结构为

$$Z(f)=\{1\}+\frac{q^m-1}{e}\{e\}+\frac{q^{pm}-q^m}{ep}\{ep\}+\frac{q^{p^2m}-q^{pm}}{ep^2}\{ep^2\}+\cdots+\frac{q^{p^\lambda m}-q^{p^{\lambda-1}m}}{ep^\lambda}\{ep^\lambda\}+\frac{q^n-q^{p^\lambda m}}{ep^{\lambda+1}}\{ep^{\lambda+1}\}.$$

(2) 若$f(x)=f_1(x)\cdots f_s(x)$,其中,$f_1,\cdots,f_s$为$\mathbf{F}_q[x]$中两两互素的多项式.则

$$Z(f)=Z(f_1)\odot Z(f_2)\odot\cdots\odot Z(f_s).$$

证明 (1) $S(f)$中每个序列$\underline{a}$对应真分式$A(x)=\dfrac{h(x)}{f(x)}=\dfrac{h(x)}{g(x)^b}$.将它化为既约真分式则为

$$A(x)=\frac{k(x)}{g(x)^{b'}},\qquad 0\leqslant b'\leqslant b,\quad g(x)\nmid k(x).$$

由于次数小于$\deg g(x)^{b'}=mb'$的$k(x)$共有$q^{mb'}$个,而其中$g(x)\mid k(x)$的共有$q^{m(b'-1)}$个.于是以$g(x)^{b'}$为分母的既约真分式共有$q^{mb'}-q^{m(b'-1)}$个.由定理2.6.3,它们对应序列的周期等于$g(x)^{b'}$的周期.再由定理1.5.8,$g(x)^{b'}$的周期为$ep^{t'}$,其中t'是满足$p^{t'}\geqslant b'$的最小整数.

当$b'=0$时,$A(x)=\dfrac{0}{1}$对应全零序列,对于周期结构的贡献为$\{1\}$.

当 $b'=1$时，$t'=0$. 周期为 e，共 q^m-1个序列，对于周期结构的贡献为$\frac{q^m-1}{e}\{e\}$.

当 $b'=2,3,\cdots,p$ 时，$t'=1$，序列的周期均为 ep，共有 $\sum_{b'=2}^{p}(q^{mb'}-q^{(b'-1)m})=q^{pm}-q^m$ 个序列. 对于周期结构的贡献为 $\frac{q^{pm}-q^m}{ep}\{ep\}$.

当 $b'=p+1,\cdots,p^2$时，$t'=2$，序列的周期均为 ep^2，共有 $\sum_{b'=p+1}^{p^2}(q^{mb'}-q^{m(b'-1)})=q^{p^2m}-q^{pm}$个序列. 对于周期结构的贡献为 $\frac{q^{p^2m}-q^{pm}}{ep^2}\{ep^2\}$.

……

当 $t'=\lambda$ 时，$b'=p^{\lambda-1}+1,\cdots,p^\lambda$，对于周期结构的贡献为 $\frac{q^{p^\lambda m}-q^{p^{\lambda-1}m}}{ep^\lambda}\{ep^\lambda\}$. 最后，当 $t'=\lambda+1$时，$b'=p^\lambda+1,\cdots,n$. 对周期结构的贡献为$\frac{q^n-q^{p^\lambda m}}{ep^{\lambda+1}}\{ep^{\lambda+1}\}$. 将所有贡献加在一起，便给出 $S(f)$的周期结构 $Z(f)$.

(2)　不妨设 $s=2$（用数学归纳法即可证明一般情形），即设 $f(x)=f_1(x)f_2(x)$，其中 f_1和 f_2互素. 先证每个真分式$A(x)=\frac{g(x)}{f(x)}$可唯一表示成

$$\frac{g(x)}{f(x)}=\frac{g_1(x)}{f_1(x)}+\frac{g_2(x)}{f_2(x)} \tag{8}$$

其中右边为两个真分式之和. 这种表达式的存在性是由于 f_1和 f_2互素，从而有 $h(x),k(x)\in F_q[x]$，使得

$$h(x)f_1(x)+k(x)f_2(x)=1. \quad \text{于是}$$

$$g(x)h(x)f_1(x)+g(x)k(x)f_2(x)=g(x). \quad (9)$$

用 f_2除 $g(x)h(x)$得到

$$g(x)h(x)=q(x)f_2(x)+g_2(x), \deg g_2(x)<\deg f_2(x),$$

则(9)式为

$$g(x)=g_2(x)f_1(x)+g_1(x)f_2(x), \quad (10)$$

其中 $g_1(x)=gk-qf_1$. 由 $\deg g(x)<\deg f(x)=\deg f_1+\deg f_2$, $\deg g_2 f_1<\deg f_1+\deg f_2$. 可知 $\deg g_1 f_2=\deg(g-g_2 f_1)<\deg f_1 f_2$. 于是 $\deg g_1<\deg f_1$. 将(10)式两边除以 $f=f_1 f_2$即得(8)式,并且$\frac{g_1}{f_1}$和$\frac{g_2}{f_2}$均为真分式.

再证分解式(8)的唯一性:若又有

$$\frac{g(x)}{f(x)}=\frac{g_1'}{f_1}+\frac{g_2'}{f_2},$$

其中右边为两个真分式之和. 将此式减去(8)式,给出$\frac{g_1'-g_1}{f_1}=-\frac{g_2'-g_2}{f_2}$. 即$(g'_1-g_1)f_2=-f_1(g_2'-g_2)$. 由于$(f_1,f_2)=1$,从而 $f_2|g_2'-g_2$. 但是 $\deg(g_2'-g_2)<\deg f_2$. 从而必然 $g_2'=g_2$. 于是 $g_1'=g_1$. 这就证明了(8)式唯一性.

(8)式左边有 q^n 个可能,而右边(即 $\deg g_1<\deg f_1$, $\deg g_2<\deg f_2$条件下)也有 $q^{\deg f_1}\cdot q^{\deg f_2}=q^{\deg f}=q^n$ 个可能,从而 $S(f_1)$中序列$\underline{a}$和 $S(f_2)$中序列$\underline{a'}$相加得出 $S(f)$中序列,并且由此得到$S(f)$中全部序列.(这里序列$\underline{a}=a_0a_1\cdots$和$\underline{a}'=a_0'a_1'\cdots$相加是指序列$\underline{a}+\underline{a'}$的第 n 位为 $a_n+a_n'(n=0,1,2,\cdots,)$).

设$\{P\}$是 $Z(f_1)$中一个周期为 P 的序列平移等价类,$\underline{a}$为其中一个序列.$\{Q\}$是 $Z(f_2)$中一个周期为 Q 的平移等价类,$\underline{b}$为其中一个序列. 我们证明序列$\underline{a}+\underline{b}$的周期为$[P,Q]$(最小公倍数). 这是由于$\underline{a}$和$\underline{b}$分别对应既约真分式

$$A_1(x)=\frac{g_1'}{f_1'},A_2(x)=\frac{g_2'}{f_2'},$$

其中 $f_1'|f_1, f_2'|f_2$. 由于$(f_1,f_2)=1$，从而$(f_1',f_2')=1$. 并且$\underline{a}$和$\underline{b}$的周期分别为 $P=p(f_1')$ 和 $Q=p(f_2')$. 易证

$$A_1(x)+A_2(x)=\frac{g_1'f_2'+g_2'f_1'}{f_1'f_2'}$$

已经是既约的了(如果有 $F_q[x]$中某个不可约多项式 $p(x)$除尽分子和分母，不妨设 $p(x)|f_1'$，则 $p(x)|g_1'f_2'$. 由于$(f_1',f_2')=1$，所以 $p(x)\nmid f_2'$，于是 $p(x)|g_1'$. 这就与$\frac{g_1'}{f_1'}$是既约的相矛盾). 所以序列$\underline{a}+\underline{b}$的周期为 $p(f_1f_2)=[p(f_1'),p(f_2')]=[P,Q]$ (定理1.5.8的(4)). 这就表明:$\{P\}$中每个序列$\underline{a}$和$\{Q\}$中每个序列上相加得到$S(f)$中序列的周期为$[P,Q]$的一个序列. 但是$[P]$和$[Q]$中分别有 P 和 Q 个序列. 它们共给出 $Z(f)$中 PQ 个序列，每个序列的周期均为$[P,Q]$，从而对 $Z(f)$的贡献为$\frac{PQ}{[P,Q]}\{[P,Q]\}=(P,Q)\{[P,Q]\}=[P]\odot[Q]$(这就是为什么 R 中乘法$\odot$如此定义!). 再由分配律，便知 $Z(f)=Z(f_1)\odot Z(f_2)$ 证毕.

例3 设 $f(x)=(x^2+x+1)^3(x^4+x+1)\in F_2[x]$. 取 $f_1=(x^2+x+1)^3$，$f_2=(x^4+x+1)$. 由于 x^2+x+1的周期为3. 由定理2.6.8的(1)可知

$$\begin{aligned}Z(f_1)&=\{1\}+\frac{2^2-1}{3}\{3\}+\frac{2^4-2^2}{6}\{6\}+\frac{2^6-2^4}{12}\{12\}\\&=\{1\}+\{3\}+2\{6\}+4\{12\}.\end{aligned}$$

由于 f_2为本原多项式，从而 $Z(f_2)=\{1\}+\{15\}$. 于是

$$\begin{aligned}Z(f)&=Z(f_1)\odot Z(f_2)\\&=(\{1\}+\{3\}+2\{6\}+4\{12\})\odot(\{1\}+\{15\})\\&=\{1\}+\{3\}+2\{6\}+4\{12\}+\{5\}+\{15\}+6\{30\}\end{aligned}$$

$+12\{60\}$

$=\{1\}+\{3\}+2\{6\}+4\{12\}+4\{15\}+6\{30\}+12\{60\}.$

2.6.9 习　题

1. 一个 q 元序列$\underline{a}=a_0a_1\cdots a_n\cdots(a_i\in F_q)$叫作拟周期序列，是指存在整数 $N\geqslant 0$和正整数 P，使得当 $n\geqslant N$ 时，$a_{n+p}=a_n$. 满足此条件的最小整数 N 和 P 分别叫作拟周期序列$\underline{a}$的不循环位数和周期.（当 $N=0$时，$\underline{a}$即为周期序列）. 求证：

   (1) $\underline{a}$为拟周期序列$\Longleftrightarrow A(x)=a_0+a_1x+\cdots+a_nx^n+\cdots$

   可表成分式
   $$A(x)=\frac{g(x)}{f(x)},$$
   其中 $f(x),g(x)\in F_q[x]$，　$f(0)\neq 0$.

   (2) 如果 $A(x)=\frac{g(x)}{f(x)}$为既约分式，$f(0)\neq 0$. 则拟周期序列$\underline{a}$的周期为 f 的周期，而$\underline{a}$的不循环位数为
   $$N=\max\{0,\deg g(x)-\deg f(x)+1\}.$$

2. 构作一个2级5元 M 序列.

3. 对于 $F_3[x]$中多项式 $f(x)=(1+x^2)^5(1+x+2x^2)$，求 $S(f)$的周期结构 $Z(f)$.

4. 设 $f(x)=f_1(x)f_2(x)$，其中 $f_1(x)=1+x+x^3$和 $f_2(x)=1+x$ 均是 $F_2[x]$中多项式.

   (1) 求证以01111 001000011为一个周期节的二元序列属于 $S(f)$.

   (2) 将上述序列分解成两个序列$\underline{a}$和$\underline{b}$之和，使得$\underline{a}\in S(f_1)$，$\underline{b}\in S(f_2)$.

5. 设 $f(x)=(1+x+x^2)^2\in F_2[x]$. 试问 $S(f)$中共有多少个序列的平移等价类？每个平移等价类的周期是多少？对每个平移等价类构作出其中一个序列来.

§ 2.7 q 元序列(续)

上节表明,给了 $F_q[x]$中一个本原多项式 $f(x)$,$S(f)$中本质上只有一个非零序列(即 $S(f)$中所有非零序列均彼此平移等价),将此非零序列一个周期节中 $n-1$个0相连的地方增加一个0,便得到一个 n 级 q 元 M 序列,由于周期节中共有 $q-1$个地方有连续 $n-1$个0(它们分别对应于状态$0\ 0\cdots0\ a, a\in F_q^*$),所以共可作成 $q-1$个 M 序列,我们在第1.5节中知道,$F_q[x]$中共有 $\frac{1}{n}\varphi(q^n-1)$个 n 次本原多项式. 因此用这种方法共作出

$$\frac{q^n-1}{n}\varphi(q^n-1)\left(<\frac{1}{n}q^{2n}\right)$$

个 n 级 q 元 M 序列. 但是我们说过,n 级 q 元 M 序列一共有

$$((q-1)!)^{q^{n-1}}q^{q^{n-1}-n}$$

个. 将这两个数相比较,可知采用上节方法得到的 M 序列毕竟是其中的一小部分. 由于 M 序列的重要实用价值,寻求构作 M 序列的其他方法,是保密通信当中的一个有现实意义的研究课题. 近年来,许多数学家(包括我国数学家)在这方面作了很多工作. 但是本文不打算深入介绍这些工作,因为研究工具以图论为主,超出了本书的范围. 有兴趣的读者可参看万哲先等人所写《非线性移位寄存器》一书和其他有关文献.

我们继续讲述 $S(f)$中的序列. 对于给定的 $F_q[x]$中 n 次多项式 $f(x)$,$S(f)$中的序列都是线性递归序列,即序列的每位可由它前面的 n 位线性地表达出来(即第2.6节的公式(5)). 这种线性递归序列在技术上用一种叫作"线性移位寄存器"的设备很容易实现,这是它们的一个很大的优点.

如果 $f(x)$ 是 n 次本原多项式，则 $S(f)$ 中的非零序列还有其他好的特性. 不仅用它们来构作 M 序列，而这些序列本身在通信中有许多其他用途，所以有必要给它们起如下的名称

2.7.1 定义 设 $f(x)$ 是 $F_q[x]$ 中 n 次本原多项式，则以 $f(x)$ 为生成多项式得到的 $S(f)$ 中(唯一的)非零序列叫作 n级 q 元 m序列.

现在我们列举 m 序列的一些特性. 首先，n 级 q 元 m 序列是周期为 q^n-1 的序列，它的连续 q^n-1 个状态

$$a_i a_{i+1} \cdots a_{i+n-1} \quad (0 \leqslant i \leqslant q^n-2)$$

恰好是由 F_q 中元素作成的全部 q^n-1 个非零状态. 由此出发我们可以得到

2.7.2 定理 (m 序列元素分布特性) 设 $\underline{a}$ 是 n 级 q 元 m 序列.

(1) 对每个 k，$1 \leqslant k \leqslant n$ 和 F_q 中任意不全为零的 k 个元素 c_1，c_2，$\cdots c_k$，在 $\underline{a}$ 的一个首尾相连的周期节中共有 q^{n-k} 个 $c_1 \cdots c_m$. 当 $1 \leqslant k \leqslant n-1$ 时，共有 $q^{n-k}-1$ 个地方有连续 k 个0. 但是当 $k \geqslant n$ 时，不存在连续 k 个0. 当 $k \geqslant n+1$ 时，不存在连续 k 个 g (对每个 $g \in F_q^*$).

特别地，在 $\underline{a}$ 的一个周期节中有 $q^{n-1}-1$ 个0，而对每个 $g \in F_q^*$，共有 q^{n-1} 个 g.

证明 设 $1 \leqslant k \leqslant n$，$c_1 \cdots c_k$ 为 F_q 中 k 个不全为零的元素. 在 $\underline{a}$ 的一个周期节里，每出现 $c_1 \cdots c_k$，均把它看作是某个状态 $a_i a_{i+1} \cdots a_{i+n-1}$ 的前 k 位. 由于以 $c_1 \cdots c_k$ 为前 k 位的状态共有 q^{n-k} 个. 所以 $\underline{a}$ 的周期节中 $c_1 \cdots c_k$ 共出现 q^{n-k} 个. 当 $1 \leqslant k \leqslant n-1$ 时，前 k 位均

为零的非零状态共有 $q^{n-k}-1$ 个. 所以 $\underline{a}$ 的周期节中共有 $q^{n-k}-1$ 处出现连续 k 个0. 而 $k \geqslant n$ 时, 若 $\underline{a}$ 的某处有连续 k 个0, 由于 $\underline{a}$ 是 n 级线性递归序列, 可知 $\underline{a}$ 必然为全零序列, 但作为 m 序列 $\underline{a}$ 不能为全零序列, 所以当 $k \geqslant n$ 时, $\underline{a}$ 中不存在连续 k 个0. 同理可证当 $k \geqslant n+1$ 时, $\underline{a}$ 中不存在连续 k 个 g(对每个 $g \in F_q^*$). 否则 $\underline{a}$ 就成为所有数字均为 g 的序列了, 证毕.

定理2.7.2表明 m 序列中 F_q 的每个元素和元素段的分布非常均衡, 并且没有较长一段均是同样的元素. 这种序列加在原始信息序列上, 可以把原来序列变得面目全非. 所以适用于作加密用.

m 序列的另一个好的性能是自相关特性. 为简单起见我们只考虑 p 元序列, 即 q 为素数 p 的情形.

2.7.3 定义 设 p 为素数, $\underline{a}=a_0a_1\cdots$ 是周期为 l 的 p 元序列($a_i \in F_p$), 令 $\zeta = e^{\frac{2\pi i}{p}}$. 对每个 t, $0 \leqslant t \leqslant p-1$, 令

$$c_t = c_t(\underline{a}) = \sum_{i=0}^{l-1} \zeta^{a_{i+t}-a_i} = \sum_{i=0}^{l-1} \zeta^{a_{i+t}} \bar{\zeta}^{a_i}.$$

称 $c_0, c_1 \cdots, c_{l-1}$ 为 p 元序列 $\underline{a}$ 的**自相关值**. 显然

$$c_0 = \sum_{i=0}^{l-1} \zeta^{a_i - a_i} = \sum_{i=0}^{l-1} 1 = l.$$

即 c_0 等于序列 $\underline{a}$ 的周期, 它叫作 $\underline{a}$ 的自相关**主值**, 而 $c_1, c_2, \cdots, c_{l-1}$ 叫作 $\underline{a}$ 的自相关**非主值**.

在通信系统中, 需要构作自相关性能良好的序列. 所谓自相关性能良好, 即指所有自相关非主值的绝对值与自相关主值(即序列的周期 l)相比均要小很多. 下面定理表明, m 序列是自相关性能非常好的序列, 所以广泛地用于同步通信系统中.

2.7.4 定理 n 级 p 元 m 序列 $\underline{a}$ 的所有自相关非主值均为 -1.

证明 m 序列 $\underline{a}$ 的周期为 $l=p^n-1$. 令 $b_i=a_{i+t}-a_i(i=0,1,2,\cdots)$, 则序列 $\underline{b}=b_0b_1\cdots$ 等于 $L^t\underline{a}-\underline{a}$. 当 $1\leqslant t\leqslant l-1$ 时, $L^t\underline{a}\neq\underline{a}$. 从而 $\underline{b}$ 不是全零序列. 另一方面, 由于 $\underline{a}\in S(f)$, 其中 $f(x)$ 为 $\boldsymbol{F}_p[x]$ 中 n 次本原多项式. 而 $L^t\underline{a}\in S(f)$(定理2.6.6), 从而 $\underline{b}=L^t\underline{a}-\underline{a}$ 也属于 $S(f)$. (这是由于 $L^t\underline{a}$ 和 $\underline{a}$ 的幂级数以 $f(x)$ 为分母, 所以 $\underline{b}=L^t\underline{a}-\underline{a}$ 也如此) 即 $\underline{b}$ 为 $S(f)$ 中非零序列, 因此 $\underline{b}$ 也是一个 n 级 p 元 m 序列. 于是在 $\underline{b}$ 的一个周期节中共有 $p^{n-1}-1$ 个0, 而对每个 $g\in\boldsymbol{F}_p^*$, 共有 p^{n-1} 个 g. 因此对每个 $1\leqslant t\leqslant l-1$ ($\zeta=e^{\frac{2\pi i}{p}}$),

$$
\begin{aligned}
c_t(\underline{a})&=\sum_{i=0}^{l-1}\zeta^{a_{i+t}-a_i}=\sum_{i=0}^{l-1}\zeta^{b_i}\\
&=p^{n-1}\cdot\sum_{g\in\boldsymbol{F}_p^*}\zeta^g+(p^{n-1}-1)\cdot\zeta^0\\
&=p^{n-1}\sum_{g\in\boldsymbol{F}_p}\zeta^g-1=p^{n-1}\sum_{i=0}^{p-1}\zeta^i-1=-1.
\end{aligned}
$$

这就证明了定理2.7.4(最后等式我们利用了恒等式 $1+\zeta+\zeta^2+\cdots+\zeta^{p-1}=\frac{1-\zeta^p}{1-\zeta}=0$).

在通信系统中最常用的是二元序列, 即序列 $\underline{a}=a_0a_1\cdots a_n\cdots$ 中每个元素为0或1(它代表开关线路的"开"和"关"两个状态), 这时 $p=2$, $\zeta_2=e^{\frac{2\pi i}{2}}=-1$. 若 $\underline{a}$ 的周期为 l, 则 $\underline{a}$ 的自相关值为

$$
c_t(\underline{a})=\sum_{i=0}^{l-1}(-1)^{a_{i+t}-a_i}=\sum_{\substack{i=0\\a_{i+t}=a_i}}^{l-1}1-\sum_{\substack{i=0\\a_{i+t}\neq a_i}}^{l-1}1. \tag{1}
$$

换句话说, 对每个 $1\leqslant t\leqslant l-1$. 将 $\underline{a}$ 和 $L^t\underline{a}$ 两个序列的一个周期

节排在一起：

$$\underline{a} = a_0 a_1 a_2 \cdots a_i \cdots a_{l-1}$$

$$L^t\underline{a} = a_t a_{t+1} a_{t+2} \cdots a_{i+t} \cdots a_{t+l-1}$$

如果第 i 位处 a_i 和 a_{i+t} 相同（即均为0或均为1），称此位为 $\underline{a}$ 和 $L^t\underline{a}$ 的相同位，若 a_i 和 a_{i+t} 不同（即一为0另一为1），则此位叫作 $\underline{a}$ 和 $L^t\underline{a}$ 的相异位. 由(1)式可知，$\underline{a}$ 的自相关值 $c_t(\underline{a})$ 等于 $\underline{a}$ 和 $L^t\underline{a}$ 的相同位数减去相异位数. 一个二元周期序列 $\underline{a}$ 具有好的自相关性能，即指对每个 $1 \leqslant t \leqslant l-1$（$l$ 为 $\underline{a}$ 的周期），$\underline{a}$ 和 $L^t\underline{a}$ 的相同位数和相异位数相差无几. 而对于二元 m 序列 $\underline{a}$，对每个 $1 \leqslant t \leqslant l-1$（$l = 2^n - 1$，$n$ 为 m 序列 $\underline{a}$ 的级数），$\underline{a}$ 和 $L^t\underline{a}$ 的相同位数均比相异位数少1.

例1 对于第2.6节开头所举的4级二元 m 序列 $\underline{a}$，这是周期15的序列. 它的前15位为

$$\underline{a} = 010110010001111\cdots$$

将 $\underline{a}$ 和 $L^3\underline{a}$ 的前15位对齐：

$$\underline{a} = 010110010001111\cdots$$

$$L^3\underline{a} = 110010001111010\cdots$$

发现它们的相同位有7个，相异位有8个. 于是 $c_3(\underline{a}) = 7 - 8 = -1$. 类似地，对每个 $1 \leqslant t \leqslant 14$，$\underline{a}$ 和 $L^t\underline{a}$ 的前15位当中均有7个相同位和8个相异位，即自相关非主值均为 -1.

构作自相关性能良好二元序列的另一种办法是用差集合.

2.7.5 定理 设 $D = \{d_1, d_2, \cdots, d_k\}$ 为参数 (v, k, λ) 的差集合，如下定义周期为 v 的二元序列 $\underline{a} = a_0 a_1 \cdots a_{v-1} \cdots$，其中

$$a_i = \begin{cases} 0, & 若\ i \in D \\ 1, & 否则 \end{cases}$$

则序列 $\underline{a}$ 所有自相关函数非主值均为 $v - 4k + 4\lambda$.

证明 对于$1\leqslant t\leqslant v-1$，

$$c_t(\underline{a})=\sum_{\substack{i=0\\a_{i+t}=a_i=0}}^{v-1}1+\sum_{\substack{i=0\\a_{i+t}=a_i=1}}^{v-1}1+\sum_{\substack{i=0\\a_{i+t}\neq a_i}}^{v-1}(-1).$$

根据差集合的定义，共有λ个i，使得$i+t$和i均属于D，即$a_{i+t}=a_i=0$. 再由于D中共有k个元素，从而共有$k-\lambda$个i使得$i+t\in D,i\notin D$. 也有$k-\lambda$个i使得$i+t\notin D,i\in D$. 对于这$2(k-\lambda)$个i，$a_{i+t}\neq a_i$. 最后，剩下的$v-\lambda-2(k-\lambda)=v-2k+\lambda$个$i$满足$i\notin D,i+t\notin D$，即$a_{i+t}=a_i=1$. 因此

$$\begin{aligned}c_t(\underline{a})&=\lambda+(v-2k+\lambda)-2(k-\lambda)\\&=v-4k+4\lambda.\ (1\leqslant t\leqslant v-1).\end{aligned}$$
证毕.

例2 定理2.4.4给出 Singer 差集合，其参数为$(v,k,\lambda)=\left(\frac{q^{n+1}-1}{q-1},\frac{q^n-1}{q-1},\frac{q^{n-1}-1}{q-1}\right)$，其中$q$为素数幂. 利用这种差集合构作出周期为$\frac{q^{n+1}-1}{q-1}$的二元序列，其自相关非主值均为$\frac{1}{q-1}[q^{n+1}-1-4(q^n-q^{n-1})]=\frac{q^{n+1}-1}{q-1}-4q^{n-1}$. 特别地，取$q=2$，则得到周期为$2^{n+1}-1$的二元序列，其自相关非主值均为$-1$. 这和$m$序列有同样的周期和同样好的自相关性能.

例3 对于素数$p\equiv3 \pmod 4$，定理2.5.6构作出参数$(v,k,\lambda)=\left(p,\frac{p-1}{2},\frac{p-3}{4}\right)$的差集合. 再用定理2.7.5给出周期为$p$的二元序列，其自相关非主值均为$p-4\cdot\left(\frac{p-1}{2}-\frac{p-3}{4}\right)=-1$. 这种序列有与$m$序列同样好的自相关性能，并且周期值$p$选取范围比$m$序列更广，因为$m$序列的周期只能是形如$2^n-1$的数. 根据定理2.5.6中差集合的构作方式，我们知道二元序列$\underline{a}=a_0a_1\cdots a_{p-1}\cdots(p\equiv3 \pmod 4)$为：对于$0\leqslant i\leqslant p-1$，

$$a_i=\begin{cases}0, & \text{若 } i \text{ 为模 } p \text{ 的非二次剩余}\\ 1, & \text{否则}\end{cases}$$

例如取 $p=19$，差集合为 $D=\{2,3,8,10,12,13,14,15,18\}$（即模19的非二次剩余全体）．而 $\underline{a}$ 的一个周期节为

1100111101010000110.

以上我们构作的自相关性能良好的二元序列，其周期均是奇数．作为本书的结尾，我们向大家介绍 A. Lempel，M. Cohn 和 W. L. Eastman 于1977年构作的自相关性能良好的二元序列，其周期为偶数（文章为 *A class of Balanced Binary Sequences with Optimal Autocorrelation Properties*，IEEE Trans. on Imformation Theory，IT—23(1977)，38—42）．

2.7.6 定理 设 q 为奇素数的幂，令 α 为 F_q 的一个本原元素（于是 $F_q^*=\{1,\alpha,\alpha^2,\cdots,\alpha^{q-2}\}$，如下定义周期为 $q-1$ 的二元序列 $\underline{a}=a_0a_1\cdots a_{q-2}\cdots$，其中

$$a_i=\begin{cases}0, & \text{若 } \alpha^i+1 \text{ 为 } F_q \text{ 中非平方元素}\\ 1, & \text{否则}\end{cases}$$

则当 $q-1\equiv 2 \pmod 4$ 时，序列 $\underline{a}$ 的自相关非主值均为 ± 2．而当 $q-1\equiv 0 \pmod 4$ 时，序列 $\underline{a}$ 的自相关非主值为0或 -4．

证明 （这里的证明比原文大大简化）．对于 $c\in F_q$，定义

$$f(c)=\begin{cases}1, & \text{若 } c \text{ 为 } F_q^* \text{ 中平方元素}\\ -1, & \text{若 } c \text{ 为 } F_q^* \text{ 中非平方元素}\\ 0, & \text{若 } c=0\end{cases}$$

那末 a_i 的定义可以写成

$$a_i=\begin{cases}0, & \text{若 } f(\alpha^i+1)=-1\\ 1, & \text{否则}\end{cases}$$

于是对$1\leqslant t\leqslant q-2$，

$$\begin{aligned}c_t(\underline{a})&=\sum_{i=0}^{q-2}(-1)^{a_i+a_{i+t}}\\&=\sum_{i=0}^{q-2}(-f(\alpha^i+1))(-f(\alpha^{i+t}+1))-f(1-\alpha^t)\\&\qquad-f(1-\alpha^{-t}).\end{aligned}$$

这是由于当 $i\neq\frac{q-1}{2},\frac{q-1}{2}-t$ 时，$\alpha^i+1\neq0$，$\alpha^{i+t}+1\neq0$. 从而 $(-1)^{a_i+a_{i+t}}=(-f(\alpha^i+1))(-f(\alpha^{i+t}+1))$. 而当 $i=\frac{q-1}{2}$ 时，$f(\alpha^i+1)=f(0)=0$，而 $(-1)^{a_i+a_{i+t}}=(-1)^0\cdot(-f(\alpha^{i+t}+1))=-f(1-\alpha^t)$. 当 $i=\frac{q-1}{2}-t$ 时，$f(\alpha^{i+t}+1)=f(0)=0$，而 $(-1)^{a_i+a_{i+t}}=(-f(\alpha^i+1))\cdot(-1)^0=-f(1-\alpha^{-t})$. 于是

$$c_t(\underline{a})=\sum_{x\in F_q^*}f(x+1)f(\alpha^t x+1)-f(1-\alpha^t)-f(1-\alpha^{-t})$$

由于 f 是积性函数，即 $f(a)f(b)=f(ab)$，$f(\alpha^t)=(-1)^t$，所以

$$\begin{aligned}c_t(\underline{a})&=f(\alpha^t)\sum_{x\in F_q^*}f(x+1)f(x+\alpha^{-t})-f(1-\alpha^t)\\&\qquad-f(-\alpha^{-t})f(1-\alpha^t)\\&=-1+(-1)^t\sum_{x\in F_q}f(x^2+(1+\alpha^{-t})x+\alpha^{-t})\\&\qquad-f(1-\alpha^t)(1+(-1)^t f(-1))\\&=-1+(-1)^t\sum_{x\in F_q}f\left[\left(x+\frac{1+\alpha^{-t}}{2}\right)^2-\left(\frac{1-\alpha^{-t}}{2}\right)^2\right]\\&\qquad-f(1-\alpha^t)(1+(-1)^t f(-1))\\&=-1+(-1)^t\sum_{x\in F_q}f(x^2-1)\\&\qquad-f(1-\alpha^t)(1+(-1)^t f(-1)).\end{aligned}\tag{2}$$

现在我们计算 $\sum\limits_{x\in F_q}f(x^2-1)$. 为此，我们考虑 $\sum\limits_{x\in F_q}f(x)=0$. 于是

$$\sum_{x,y\in F_q} f(x^2-y^2)=\sum_{x,y\in F_q} f(x+y)f(x-y)$$

(令 $A=x+y, B=x-y$)

$$=\sum_{A,B\in F_q} f(A)f(B)=\Big(\sum_{A\in F_q} f(A)\Big)^2$$

$$=0.$$

另一方面,

$$\sum_{x,y\in F_q} f(x^2-y^2)=\sum_{x\in F_q} f(x^2)+\sum_{y\in F_q} f(-y^2)+\sum_{x,y\in F_q^*} f(x^2-y^2)$$

$$=(q-1)+(q-1)f(-1)+(q-1)\sum_{x\in F_q^*} f(x^2-1)$$

于是 $$\sum_{x\in F_q^*} f(x^2-1)=-1-f(-1).$$

从而 $\sum_{x\in F_q} f(x^2-1)=-1$. 代入(2)式得到

$$c_t(\underline{a})=-1+(-1)^{t+1}-f(1-\alpha^t)(1+(-1)^t f(-1)).$$

若 $q-1\equiv 2 \pmod 4$, 则 $\frac{q-1}{2}$ 为奇数. 所以 $-1=\alpha^{\frac{q-1}{2}}$ 是非平方元素, 即 $f(-1)=-1$. 于是

$$c_t(\underline{a})=-1+(-1)^{t+1}\pm(1+(-1)^{t+1})$$

$$=\begin{cases}-2 & \text{当} 2|t \text{ 时}\\ \pm 2 & \text{当} 2\nmid t \text{ 时}\end{cases}$$

若 $q-1\equiv 0 \pmod 4$, 则 $f(-1)=1$, 于是

$$c_t(\underline{a})=-(1+f(1-\alpha^t))(1+(-1)^t)=0\text{或}-4.$$

这就证明了定理2.7.6.

例4 取 $q=17$, 则 $\alpha=3$ 为模17的原根(本原元素). F_{17}^* 中16

个元素为

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
(mod 17) 3^i	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6

用定理2.7.6构作的二元序列 $\underline{a}$ 的周期为16. 前16位为 $a_0a_1\cdots a_{15}=1100001011110100$. 其自相关非主值为 $c_t(\underline{a})=-4$(对于 $t=4,6,10,12$),$c_t(\underline{a})=0$(对于 $t=1,2,3,5,7,8,9,11,13,14,15$).

例5 $q=3^3$. $\boldsymbol{F}_q=\boldsymbol{F}_3(\alpha)$,$\alpha^3=\alpha+2$. 则 α 为 $\boldsymbol{F}_q$ 中本原元素,设 $\alpha^i=c_0+c_1\alpha+c_2\alpha^2$,$c_i\in\boldsymbol{F}_3$. 利用定理2.7.6构作出周期26的二元序列 $\underline{a}$,它的前26位为

$$a_0a_1\cdots a_{25}=00001001001111101100011101.$$

它的自相关非主值为±2.

2.7.7 习 题

1. 试参考 m 序列的元素分布特性(定理2.7.2)来研究 M 序列的元素分布特性.
2. 设 $\underline{a}$ 是 n 级 q 元 M 序列. 求证当 $1\leqslant t\leqslant n-1$ 时 $c_t(\underline{a})=0$.
3. 设 p 为素数,$p\equiv1 \pmod 4$. 定义周期为 p 的二元序列 $\underline{a}$,$\underline{a}$ 的前 p 位数字 $a_0a_1\cdots a_{p-1}$ 为

$$a_i=\begin{cases}1, & \text{若 } i \text{ 为模 } p \text{ 的非平方剩余},\\ 0, & \text{否则},\end{cases}$$

求证对于 $1\leqslant t\leqslant p-1$,

$$c_t(\underline{a})=\begin{cases}-3, & \text{若 } t \text{ 为模 } p \text{ 的非平方剩余}.\\ 1, & \text{若 } t \text{ 为模 } p \text{ 的平方剩余}.\end{cases}$$

第三章　通信网络

我们在第二章中介绍了有限域的各种应用，这一章我们专门介绍有限域在通信系统中的一个应用：如何用有限域来构作性能良好的通信网络．一个通信网络是多个地址之间的通信联系．它可以有各种各样的具体形式，如电话网络（通信地址为电话机，信息联系用电话线），电报系统，计算机信息加工和传输网络或者是人体的神经网络等．在数学上，一个通信网络可以用一个图形象地表示出来．我们首先介绍什么是通信网络以及一个性能良好的通信网络的判别标准是什么．这就需要图论中的一些术语．然后我们介绍如何构作性能良好的通信网络．这里除了用有限域之外，还需要线性代数的基本知识（包括矩阵乘法，方阵的相似性，特征根和特征向量等知识）．

§3.1　什么是通信网络？

以电话系统为例．假设有 n 个通信地址，我们用 n 个**顶点**来表示它们．如果地址 A 可以和地址 B 直接互通电话（有电话线

相连），我们便在顶点 A 和 B 之间引一条线，叫作以 A 和 B 为两端的一条边，这条边表示成$\overline{AB}$. 于是，由 n 个顶点和某些顶点之间相连的一些边，就形象地表示出一个电话系统. 在数学上，这叫作是具有 n 个顶点的图. 图4即是具有六个顶点和五条边的一个图.

今后我们总假定任意两个顶点之间至多有一条边.

我们再介绍与通信系统有关的一些图论的术语. 设 G 是一个图，A 为其中一个顶点. 如果图 G 中以 A 为端的边共有 k 条，它们是

$$\overline{AB_1},\quad \overline{AB_2},\quad \cdots,\overline{AB_k},$$

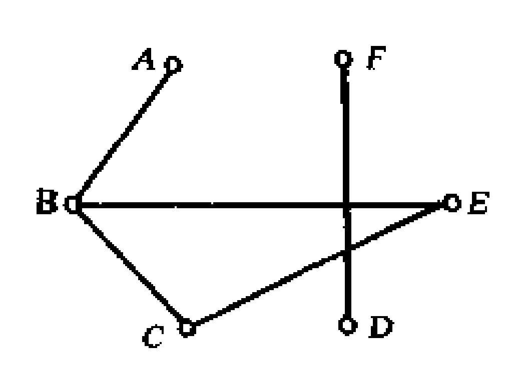


图4

则称顶点 A 的次数是 k，而顶点 $B_1, B_2\cdots, B_k$ 叫作顶点 A 的邻居. 例如图4中顶点 B 的次数为3，它的邻居为 A、C 和 E，这表示地址 B 可以与地址 A，C，E 互通电话，但是 B 不可与 D、F 互通电话.

设想图4中顶点 A 有某件事情要告诉别人. 打一次电话给 B，然后 B 再打一次电话给 E，经过两次电话，E 便得知此事. 首尾相接的两条边$\overline{AB}$和$\overline{BE}$组成长为2的一条路. 一般地，图 G 中以顶点 A 和 B 为两端的长为 d 的一条路是指 G 中首尾相接的 d 条边

$$\overline{V_1V_2},\ \overline{V_2V_3},\ \overline{V_3V_4},\ \cdots,\ \overline{V_dV_{d+1}},$$

其中 $V_1=A$，$V_{d+1}=B$. 这条路也简记成$\overline{V_1V_2\cdots V_{d+1}}$.

无向图 G 中若存在以顶点 A 和 B 为两端的长为 d 的路，表示 A 和 B 之间通过其他地址转接打 d 次电话可以互通信息. 在一个通信网络中，我们自然希望任意两个不同顶点均有路相连，

即一个地方的信息经过有限次打电话总可让所有其他地方均知道. 这样的图叫作**连通**的. 例如图4是不连通的,因为顶点 A 和 F 之间不存在路,即彼此不能互通信息. 而图5是连通图. 连通性是通信网络的起码条件,所以今后我们只研究连通图.

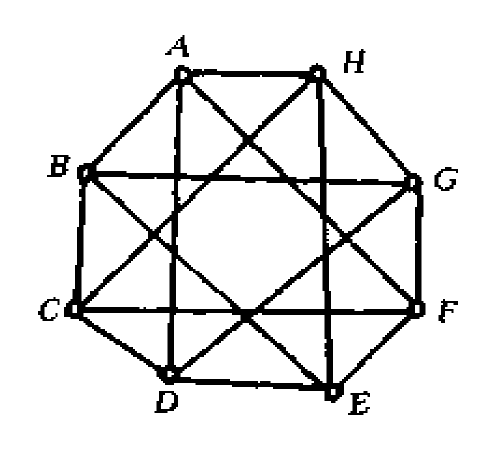


图5

设 G 是连通图. 对于 G 中两个不同顶点 v 和 v',可能有许多个不同长度的路相连. 其中最短路的长度叫作顶点 v 和 v' 之间的距离,表示成 $d(v,v')$. 例如图5中顶点 A 和 C 之间有许多条路,如 $\overline{ABC}$,$\overline{ADC}$,$\overline{AFEDC}$,$\overline{AHEBC}$ 等等. 其中最短路为 $\overline{ABC}$,$\overline{ADC}$,$\overline{AHC}$ 和 $\overline{AFC}$. 于是 $d(A,C)=d(C,A)=2$. 两个顶点之间的距离表示这两个地址交流信息所需的最少时间,一个连通图 G 中不同顶点之间所有距离的最大值,叫作图 G 的**直径**,表示成 $d(G)$. 即

$$d(G)=\max_{v\neq v'}\{d(v,v')\}$$

它的意义为:图 G 中每个顶点的信息经过 $d(G)$ 次传送即可到达所有其他顶点,并且 $d(G)$ 是满足此条件的最小整数. 例如图5的直径为2.

为了使问题简单,今后我们主要研究具有下述"正则"性质的图,图 G 叫作是 k 次正则图,是指 G 中每个顶点的次数均为 k,即每个顶点都恰好有 k 个邻居. 例如图5是4次正则图.

以上介绍了什么是通信网络. 那么,什么是好的通信网络呢?设计一个通信网络,主要应考虑三件事:网络的经济性、有效性和可靠性. 下面我们对此作简单的解释,并且说明它们的图论

意义.

(1)**网络的经济性** 如果 n 个通信地址中的每个均能与其他地址直接通话,这当然是最满意的方式.但这需要$\frac{1}{2}n(n-1)$条边.当 n 很大时,联接$\frac{1}{2}n(n-1)$条电话线,从成本上是很不合算的.所以从经济上考虑,我们希望有较少的边.如果通信网络是 k 次正则图,我们从经济上考虑即是希望 k 愈小愈好.

(2)**网络的有效性** 每个顶点只能向它的邻居直接发送信息.下一次邻居又可传给邻居的邻居.一个网络是有效的,要求每个顶点的信息经过有限步均能传送到所有其他顶点,并且为此所需时间愈少愈好.利用前面的图论术语,一个有效的通信网络要求它是连通图,并且直径愈小愈好.

(3)**网络的可靠性** 通信网络的另一个重要标准是希望它在工作中是可靠的,即希望在网络中某些通信地址或某些线路发生故障之后,不影响其余地址之间的通信.用图论的语言,我们希望构作出这样的图 G,使得 G 中去掉某些顶点(从而也去掉以这些顶点为端的边),或者去掉某些边之后,剩下的顶点和边构成的图仍旧是连通的.我们在这里不准备给出一个图的可靠性的严格数学定义.事实上,从工程实际的不同角度出发,可以有不同的判别标准,来衡量一个通信网络是否比另一个通信网络更可靠.

关于通信网络的这三个标准是相互制约的:一个图的边愈多,一般来说,有效性和可靠性愈好,但是经济性愈差.通常我们固定 n 和 k,而问题的提法为:

在所有 n 顶点 k 次正则连通图中,哪些是最有效的(即直径最小)?哪些是最可靠的?

近年来,人们发现一件有趣的事情,即图的有效性和可靠性

都依赖于图的另一个参数.这个参数便是我们下节要介绍的图的次根.

3.1.1 习　题

1. 设图 G 有 n 个顶点 $v_1,v_2,\cdots,v_n$ 和 m 条边.如果顶点 v_i 的次数为 $k_i(1\leqslant i\leqslant n)$.求证

$$k_1+k_2+\cdots+k_n=2m.$$

特别地,n 个顶点的 k 次正则图共有 $\frac{1}{2}kn$ 条边.

2. 设图 G 的顶点数 $\geqslant 2$.求证 G 中必有两个顶点的次数相同.
3. 若图 G 有 n 个顶点和 $n+1$ 条边,则 G 中必有顶点,其次数 $\geqslant 3$.
4. 求证:在六个地址的电话网络中,必然找到三个地址,它们或者彼此均可直接通话,或者彼此均不能直接通话.
5. n 名棋手进行比赛,每个棋手均与其中的若干人较量,并且比赛没有平局.如果不出现 v_1 胜 v_2,v_2 胜 v_3,$\cdots$,v_{k-1} 胜 v_k,而 v_k 又胜 v_1 这种情况.求证必有一人在比赛中全胜,也有某人在比赛中全负.

§3.2 图的次根

设 G 是具有 n 个顶点 $v_1,v_2,\cdots,v_n$ 的图,G 的**联系方阵**是指 n 阶方阵

$$M=M(G)=(a_{ij})_{1\leqslant i,j\leqslant n},$$

其中

$$a_{ij}=\begin{cases}1, & \text{如果图 } G \text{ 中有边} \overline{v_iv_j}\\ 0, & \text{否则}\end{cases}$$

例如对于图4,设顶点 A,B,C,D,E,F 依次为 $v_1,v_2,\cdots,v_6$,则它的联系方阵为

$$M = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

由定义易知 $a_{ij}=a_{ji}$，所以 M 是实对称方阵. 利用线性代数、群表示论和交换代数作为数学工具，通过联系方阵 $M(G)$ 的各种代数性质来研究图 G 的特性，是图论的一个很有意思的分支，叫作代数图论.

比如说，设 l 为自然数. 将 $M=M(G)$ 自乘 l 次，得到

$$M^l = (a_{ij}^{(l)}).$$

由矩阵乘法规则和 $M=M(G)$ 的定义不难看出：当 $i \neq j$ 时，$a_{ij}^{(l)}$ 恰好是 G 中以顶点 v_i 和 v_j 为两端的长为 l 的路的个数. 令

$$M + M^2 + \cdots + M^l = (c_{ij}^{(l)}),$$

则 $c_{ij}^{(l)} = a_{ij}^{(1)} + a_{ij}^{(2)} + \cdots + a_{ij}^{(l)}$（其中 $a_{ij}^{(1)} = a_{ij}$）. 如果对于 $i \neq j$，$c_{ij}^{(l)} \geqslant 1$，则这表示顶点 v_i 和 v_j 之间必有一条长度不超过 l 的路，即 $d(v_i, v_j) \leqslant l$. 如果对于任意的 $i, j(1 \leqslant i \neq j \leqslant n)$，$c_{ij}^{(l)}$ 均为正整数，即均有 $d(v_i, v_j) \leqslant l$，这表明图 G 的直径 $d(G)$ 不超过 l. 所以，图 G 是连通的，当且仅当存在自然数 l，使得方阵 $M+M^2+\cdots+M^l$ 的非主对角线上所有元素均 $\geqslant 1$. 并且在这种条件下，图 G 的直径 $d(G)$ 即是满足上述条件的最小自然数 l.

现在我们进一步利用线性代数工具. 设

$$A = (a_{ij})_{1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{bmatrix}$$

是一个 n 行 m 列的复矩阵，即矩阵中元素 a_{ij} 可以是任意复数．我们令．

$$\overline{A}=(\bar{a}_{ij})\quad(\bar{a}_{ij}\text{表示 } a_{ij}\text{的复共轭})$$

$$A^T=(a_{ji})_{1\leqslant j\leqslant m,1\leqslant i\leqslant n}$$

$$=\begin{bmatrix} a_{11} & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} & \cdots & a_{n2} \\ \cdots & \cdots & \cdots & \cdots \\ a_{1m} & a_{2m} & \cdots & a_{nm} \end{bmatrix}\quad(\text{为 } m \text{ 行 } n \text{ 列矩阵})$$

$\overline{A}$ 和 A^T 分别叫作矩阵 A 的共轭矩阵和转置矩阵．

现设 $A=(a_{ij})$ 为 n 阶复方阵．如果存在复数 α 和非零复向量 $a=(a_1,a_2,\cdots,a_n)$，使得

$$Aa^T=\alpha a^T,$$

我们就称 α 为方阵 A 的一个特征根，而 a 叫作方阵 A 对于特征根 α 的一个特征向量，熟知 n 阶方阵 A 共有 n 个特征根（考虑重数），它们恰好为 A 的特征多项式

$$\det(xI_n-A)=x^n+c_1x^{n-1}+\cdots+c_n$$

的 n 个根，这里 I_n 表示 n 阶单位方阵（即主对角元素均为1，而其余元素均为零），$\det(B)$ 表示方阵 B 的行列式．

两个复向量 $a=(a_1,\cdots,a_n)$ 和 $b=(b_1,\cdots,b_n)$ 的内积定义为

$$\langle a,b\rangle=a_1\bar{b}_1+a_2\bar{b}_2+\cdots+a_n\bar{b}_n=\sum_{i=1}^n a_i\bar{b}_i=a\bar{b}^T.$$

而向量 a 的长度定义为

$$\|a\|=\langle a,a\rangle^{\frac{1}{2}}=(a_1\bar{a}_1+\cdots+a_n\bar{a}_n)^{\frac{1}{2}}=\left(\sum_{i=1}^n|a_i|^2\right)^{\frac{1}{2}}.$$

如果 $\langle a,b\rangle=0$，称向量 a 和 b 彼此正交．（注意 $\langle a,b\rangle=\overline{\langle b,a\rangle}$．所以若 $\langle a,b\rangle=0$，则 $\langle b,a\rangle=0$．）最后，长度为1的向量叫作单位向量．

现在设 G 是 n 个顶点的图，$M=M(G)$ 是 G 的联系方阵. 则 M 是 n 阶实对称方阵. 线性代数的一个著名结果是说：每个 n 阶实对称方阵 M 的特征根均是实数. 如果 M 的 n 个实特征值为 $\alpha_1,\alpha_2,\cdots,\alpha_n$，那末必存在 n 个彼此正交的单位（复）向量 u_1，$u_2,\cdots,u_n$，使得 u_i 是 M 对于特征值 α_i 的特征向量，即

$$\|u_i\|=1,\langle u_i,u_j\rangle=0 \quad (1\leqslant i\neq j\leqslant n) \tag{1}$$

$$Mu_i^T=\alpha_i u_i^T \quad (1\leqslant i\leqslant n). \tag{2}$$

令

$$u_i=(u_{1i},u_{2i},\cdots,u_{ni})$$

$$U=(u_1^T u_2^T\cdots u_n^T)=\begin{pmatrix} u_{11} & u_{12} & \cdots & u_{1n} \\ u_{21} & u_{22} & \cdots & u_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ u_{n1} & u_{n2} & \cdots & u_{nn} \end{pmatrix}$$

由(1)式即知

$$\overline{U}^T U=\begin{pmatrix} \overline{u}_1 \\ \overline{u}_2 \\ \vdots \\ \overline{u}_n \end{pmatrix}(u_1^T u_2^T\cdots u_n^T)=I_n. \tag{3}$$

从而 U 是可逆方阵，并且它的逆为

$$U^{-1}=\overline{U}^T.$$

而由(2)式得到

$$MU=M(u_1^T u_2^T\cdots u_n^T)=(\alpha_1 u_1^T,\alpha_2 u_2^T,\cdots,\alpha_n u_n^T)$$

$$=(u_1^T u_2^T\cdots u_n^T)\begin{pmatrix} \alpha_1 & & & \\ & \alpha_2 & & \\ & & \ddots & \\ & & & \alpha_n \end{pmatrix}$$

$$=U\begin{pmatrix}\alpha_1 & & & \\ & \alpha_2 & & \\ & & \ddots & \\ & & & \alpha_n\end{pmatrix}.$$

于是
$$U^{-1}MU=\begin{pmatrix}\alpha_1 & & \\ & \ddots & \\ & & \alpha_n\end{pmatrix} \tag{4}$$

换句话说,实对称方阵均相似于对角方阵,并且相似方阵 U 可以选取使得满足(3)式.

3.2.1 引理 设 M 为 n 阶实对称方阵,$\alpha_1,\cdots,\alpha_n$ 是 M 的 n 个特征根,v_i 是 M 对于 α_i 的特征向量,并且 $v_1,v_2,\cdots,v_n$ 是彼此正交的单位向量,则

$$M=\sum_{i=1}^{n}\alpha_i u_i^T u_i.$$

证明 记上式右边 n 阶方阵为 B,则

$$Bu_j^T=\sum_{i=1}^{n}\alpha_i u_i^T u_i u_j^T=\sum_{i=1}^{n}\alpha_i u_i^T(u_i,u_j)$$
$$=\alpha_j u_j^T \quad (根据(1)式).$$

于是

$$BU=U\begin{pmatrix}\alpha_1 & & \\ & \ddots & \\ & & \alpha_n\end{pmatrix}=MU$$

由于 U 是可逆方阵,从而 $B=M$. 证毕.

3.2.2 定义 图 G 叫作是双份图,是指可以把图 G 的所有顶点分成两个集合 V_1 和 V_2,使得 G 中每条边均一端在 V_1 中而另一端在 V_2 中.

例如图5便是一个双份图，我们可以将它的八个顶点分成 $V_1=\{A,C,E,G\}$，$V_2=\{B,D,F,H\}$.

如果 G 是 k 次正则的双份图，则 G 中每条边的一端在 V_1 中而另一端在 V_2 中. 假设 G 中共有 m 条边. 由于 V_1 中每个顶点均引出 k 条边，因此 V_1 中共有 m/k 个顶点. 同样地，V_2 中也共有 m/k 个顶点. 即 V_1 和 V_2 有同样多的顶点. 特别地，G 中顶点总数必是偶数.

3.2.3 定理 (A) 设 G 是 k 次正则图，则 k 是联系方阵 $M=M(G)$ 的特征根，并且 G 是连通图的充分必要条件是 k 为 M 的单重特征根.

(B) 设 G 是 k 次正则的双份图，则 $-k$ 是联系方阵 $M=M(G)$ 的特征根，并且 G 是连通图的充分必要条件是 $-k$ 为 M 的单重特征根.

证明 (A) 如果 G 是 k 次正则图，则方阵 M 的每行均恰好有 k 个元素为1(其余为0). 记 $v=(1,1,\cdots,1)$(全1向量)，则

$$Mv^T=M\begin{pmatrix}1\\1\\\vdots\\1\end{pmatrix}=\begin{pmatrix}k\\k\\\vdots\\k\end{pmatrix}=k\begin{pmatrix}1\\1\\\vdots\\1\end{pmatrix}=kv^T.$$

这就表明 k 是 M 的特征根，并且全1向量是对应特征根 k 的特征向量，进而，如果 G 不是连通的，那末 G 的顶点集合可分拆成两部份 V_1 和 V_2，使得 G 中每条边的两端或者全在 V_1 中，或者全为 V_2 中. 即图 G 实际上是彼此没有边相连的两个图. 我们以 G_1 和 G_2 分别表示对应顶点集合为 V_1 和 V_2 的这两个图，$M_1=M(G_1)$，$M_2=M(G_2)$ 分别表示它们的联系方阵，则易知 G 的联系方阵为

$$M = M(G) = \begin{pmatrix} M_1 & 0 \\ 0 & M_2 \end{pmatrix}.$$

但是G_1和G_2均是k次正则的，从而M_1和M_2均有特征根k. 于是M至少有两个特征根为k.

最后，设G是连通的k次正则图，我们来证明k是单根. 设$a=(a_1,a_2,\cdots,a_n)$是M对于特征根k的特征向量，则

$$Ma^T = ka^T. \tag{5}$$

我们以a_j表示$a_1,\cdots,a_n$当中绝对值最大者. 由于a是非零向量，从而$a_j\neq 0$. 由(5)式可知

$$ka_j = \sum_{\substack{i \\ v_i与v_j相邻}} a_i. \tag{6}$$

由于a_j的极大性质，并且(6)式右边求和共有k项(因为共有k个顶点与v_j相邻). 从而由等式(6)即知对于每个与v_j相邻的顶点v_i，均有$a_j=a_i$. 继续下去，又知对于每个与v_i相邻的顶点v_t，又有$a_t=a_i(=a_j)$. 由于G是连通的，便知对于G中每个顶点v_i，均有$a_j=a_i$. 即$a_1=a_2=\cdots=a_n$，设这个公共值为$a(\neq 0)$，于是$v=a(1,1,\cdots,1)$. 换句话说，M对应特征值k的每个特征向量均是全1向量乘一个常数. 这表明k是M的单重特征根.

(B) 现设G是k次正则的双份图. 则G的顶点分拆成两个集合V_1,V_2，它们分别有s个顶点(顶点总数$n=2s$)，使得G中每条边均一端在V_1而另一端在V_2. 于是G的联系方阵有形式

$$M = M(G) = \begin{pmatrix} 0 & N \\ N^T & 0 \end{pmatrix}$$

其中N是s阶实方阵，并且N的每行每列均恰好有k个1(其余为0). 令$a=(1,1,\cdots,1,-1,-1,\cdots,-1)$(其中前$s$个为1，后$s$个为$-1$). 则

$$Ma^T=\begin{pmatrix}0 & N\\ N^T & 0\end{pmatrix}\begin{pmatrix}1\\ \vdots\\ 1\\ -1\\ \vdots\\ -1\end{pmatrix}=\begin{pmatrix}-k\\ \vdots\\ -k\\ k\\ \vdots\\ k\end{pmatrix}=-ka^T.$$

这表明$-k$是M的特征根，并且a是M对于特征根$-k$的特征向量. 最后，请读者仿照(A)来证明：k次正则双份图G是连通的，当且仅当$-k$是联系方阵$M(G)$的单重特征根. 证毕.

3.2.4 定义 设G是n个顶点的连通k次正则图. $k<n$.

(A) 如果G不是双份图，则$M=M(G)$的n个特征根为$\alpha_1=k,\alpha_2,\cdots,\alpha_n$，并且$\alpha_i\neq k(2\leqslant i\leqslant n)$(定理3.2.3(A)). 我们把$\alpha_2,\cdots,\alpha_n$的绝对值的最大者叫作图$G$的次根，表示成$\lambda(G)$，即

$$\lambda(G)=\max\{|\alpha_2|,|\alpha_3|,\cdots,|\alpha_n|\}$$

(B) 如果G为双份图，则$M=M(G)$的n个特征根为$\alpha_1=k,\alpha_2=-k,\alpha_3,\cdots,\alpha_n$，并且$\alpha_i\neq\pm k(3\leqslant i\leqslant n)$(定理3.2.3(B)). 我们定义图$G$的次根为

$$\lambda(G)=\max\{|\alpha_3|,|\alpha_4|,\cdots,|\alpha_n|\}.$$

对于n个顶点的连通k次正则图G，可以证明

(1) $\lambda(G)<k$(习题(1)).

(2) 若G不为完全双份图，并且$k<n$，则$\lambda(G)\geqslant 1$(习题(3)). 关于完全双份图的定义见习题(2).

近年来人们发现，次根小的连通正则图具有较小的直径，即这种图是有效性能好的通信网络. 人们还发现，用次根小的连通正则图可以构作出一系列可靠性能良好的通信网络. 这里，我们只说明如何利用连通正则图G的次根$\lambda(G)$来估计G的直径

$d(G)$.

3.2.5 定理 设 G 为具有 n 个顶点的连通 k 次正则图（$k\geqslant 2$，$n>k$），$\lambda=\lambda(G)$.

（A）（金芳蓉，1989）如果 G 不是双份图（于是 $1\leqslant\lambda(G)<k$），则

$$d(G)\leqslant\left[\frac{\log(n-1)}{\log k/\lambda}\right]+1.$$

其中对于实数 α，我们以 $[\alpha]$ 表示满足 $l\leqslant\alpha$ 的最大整数 l，叫作 α 的整数部份.

（B） 如果 G 是双份图，但不是完全双份图（于是 $1\leqslant\lambda(G)<k$），则

$$d(G)\leqslant\left[\frac{\log\frac{n-2}{2}}{\log\frac{k}{\lambda}}\right]+2.$$

证明 （A） 设 G 不是双份图. 令 $M=M(G)$ 的 n 个特征根为 $\alpha_1=k,\alpha_2,\cdots,\alpha_n$，$u_i=(u_{1i},u_{2i},\cdots,u_{ni})$ 是 M 对于特征根 α_i 的特征向量，并且 $u_1,u_2,\cdots,u_n$ 是彼此正交的单位向量. 由于 u_1 为全1向量的常数倍，因此 $u_1=\frac{1}{\sqrt{n}}(1,1,\cdots,1)$. 令 $U=(u_1^Tu_2^T\cdots u_n^T)$，则由(3)式知 $U^TU=I_n$，于是 $UU^T=I_n$，由此推出

$$\sum_{j=1}^{n}|u_{ij}|^2=1\quad(1\leqslant i\leqslant n).\tag{7}$$

根据引理3.2.1我们有 $M=\sum_{s=1}^{n}\alpha_su_s^Tu_s$，于是

$$M^2=\sum_{s,t=1}^{n}\alpha_s\alpha_tu_s^Tu_su_t^Tu_t=\sum_{s=1}^{n}\alpha_s^2u_s^Tu_s.$$

这是因为当 $s\neq t$ 时，$u_s u_t^T=\langle u_s, u_t\rangle=0$，而 $u_s u_s^T=1$. 归纳即知对每个正整数 d，

$$M^d=\sum_{s=1}^{n}\alpha_s^d u_s^T u_s.$$

以 $a_{ij}^{(d)}$ 表示方阵 M^d 在第 i 行第 j 列处的元素. 注意 n 阶方阵 $u_s^T u_s$ 第 i 行第 j 列处的元素为 $u_{is}u_{js}$. 因此(令 $\lambda=\lambda(G)$)

$$\begin{aligned}
a_{ij}^{(d)}&=\sum_{s=1}^{n}\alpha_s^d u_{is}u_{js}=k^d\left(\frac{1}{\sqrt{n}}\right)^2+\sum_{s=2}^{n}\alpha_s^d u_{is}u_{js}\\
&\geqslant\frac{k^d}{n}-\lambda^d\sum_{s=2}^{n}|u_{is}u_{js}|\\
&\geqslant\frac{k^d}{n}-\lambda^d\left(\sum_{s=2}^{n}|u_{is}^2\right)^{\frac{1}{2}}\left(\sum_{s=2}^{n}|u_{js}|^2\right)^{1/2}\\
&=\frac{k^d}{n}-\lambda^d(1-|u_{i1}|^2)^{\frac{1}{2}}(1-|u_{j1}|^2)^{\frac{1}{2}}\quad(\text{由(7)式})\\
&=\frac{k^d}{n}-\lambda^d\left(1-\frac{1}{n}\right)\quad\left(\text{因为 } u_{i1}=u_{j1}=\frac{1}{\sqrt{n}}\right).
\end{aligned}$$

当 $\left(\frac{k}{\lambda}\right)^d>n-1$，即 $d>\dfrac{\log(n-1)}{\log\frac{k}{\lambda}}$ 时，上式右边 >0. 于是对所有 i,j，$a_{ij}^{(d)}\geqslant 1$. 即 G 中任意两个顶点之间均有长为 d 的路. 于是

$$d(G)\leqslant\left[\frac{\log(n-1)}{\log\frac{k}{\lambda}}\right]+1.$$

(B) 若 G 是双份图，并且不为完全双份图. 设 $V_1=\{v_1, v_2,\cdots,v_s\}$，$V_2=\{v_{s+1},\cdots,v_{2s}\}$ $(n=2s)$，并且 G 中的每条边均一端在 V_1 而另一端在 V_2. 则 $\alpha_2=-k$，$u_2=\frac{1}{\sqrt{n}}(1,\cdots,1,-1,\cdots,-1)$. 于是，若 v_i 和 v_j 均属于 V_1 或者均属于 V_2，则 u_{j2} 和 u_{i2} 同时为 $\frac{1}{\sqrt{n}}$ 或同时为 $-\frac{1}{\sqrt{n}}$. 从而

$$
\begin{aligned}
a_{ij}^{(2d)} &= \sum_{s=1}^{n} \alpha_s^{2d} u_{is} u_{js} \\
&= \frac{k^{2d}}{n} + \frac{(-k)^{2d}}{n} + \sum_{s=3}^{n} \alpha_s^{2d} u_{is} u_{js} \\
&\geqslant \frac{2k^{2d}}{n} - \lambda^{2d} \sum_{s=3}^{n} |u_{is} u_{js}| \\
&\geqslant \frac{2k^{2d}}{n} - \lambda_s^{2d} \left(\sum_{s=3}^{n} |u_{is}|^2 \right)^{1/2} \left(\sum_{s=3}^{n} |u_{js}|^2 \right)^{1/2} \\
&= \frac{2k^{2d}}{n} - \lambda^{2d} \left(1 - \frac{2}{n} \right).
\end{aligned}
$$

从而当$\left(\frac{k}{\lambda}\right)^{2d} > \frac{n}{2} - 1$时，$a_{ij}^{(2d)} \geqslant 1$. 若 v_i 和 v_j 分别属于V_1和V_2，则 u_{i2}和 u_{j2}分别为$\frac{1}{\sqrt{n}}$和$-\frac{1}{\sqrt{n}}$，从而

$$
\begin{aligned}
a_{ij}^{(2d+1)} &= \sum_{s=1}^{n} \alpha_s^{2d+1} u_{is} u_{js} \\
&= \frac{k^{2d+1}}{n} + \frac{(-k)^{2d+1}}{(-n)} + \sum_{s=3}^{n} \alpha_s^{2d+1} u_{is} u_{js} \\
&\geqslant \frac{2k^{2d+1}}{n} - \lambda^{2d+1} \left(1 - \frac{2}{n} \right).
\end{aligned}
$$

从而当$\left(\frac{k}{\lambda}\right)^{2d+1} > \frac{n}{2} - 1$时，$a_{ij}^{(2d+1)} \geqslant 1$. 由此即知

$$
d(G) \leqslant \left[\frac{\log\left(\frac{n}{2} - 1\right)}{\log \frac{k}{\lambda}} \right] + 2. \text{证毕.}
$$

这样一来，为了构作性能良好的通信网络，我们又把注意力集中在寻求次根小的连通 k 次正则图这一问题上.

3.2.6 习 题

1. 对于连通 k 次正则图 G，求证 $\lambda(G) < k$.

2. 设图 G 的顶点集合分拆成两个子集 V_1 和 V_2，它们均各有 s 个元素($s \geqslant 1$). V_1 中每个顶点与 V_2 中每个顶点均有边相连，此外 G 中再没有其他的边. 这是一个连通 k 正则的双份图($k=s$)，叫作**完全双份图**，表示成 $K_{s,s}$. 求证：$\lambda(K_{s,s})=0$.

3. 设 G 是连通 k 次正则图($k \geqslant 1$). $k<n$(n 为 G 的顶点个数)，并且 G 中任意两个顶点之间至多有一条边. 求证当 G 不是完全双份图，则

   (A) $\lambda(G)>0$； (B) $\lambda(G) \geqslant 1$.

   (提示：可利用引理3.2.1)

4. 设 G 为 n 个顶点的 k 次正则图($k \geqslant 2$). 则

$$d(G) \geqslant \frac{\log(nk-n+1)}{\log k}-1.$$

§3.3 拉氏(Ramanujan)图

连通 k 次正则图的次根可以小到何等程度？1988年，Alon 和 Boppana 证明了：

对于任意正整数 $k \geqslant 2$ 和任意小的实数 $\epsilon>0$，不可能存在无穷多个不同的连通 k 次正则图，使得它们的次根均 $\leqslant 2\sqrt{k-1}-\epsilon$.

于是便提出如下的问题

3.3.1 问题 对于正整数 $k \geqslant 2$，是否存在无穷多个不同的连通 k 次正则图，使得它们的次根均 $\leqslant 2\sqrt{k-1}$？

为了方便起见，我们引入一个术语

3.3.2 定义 连通 k 次正则图叫作拉马努甘(Ramanujan)图(或者简称作**拉氏图**)，是指它的次根 $\leqslant 2\sqrt{k-1}$.

无穷多个不同的连通 k 次正则图叫作是一个 k 次**拉氏图族**.

于是,问题3.3.1可以叙述成:对于哪些正整数 k 存在 k 次拉氏图族?

为什么要把次根小于 $2\sqrt{k-1}$ 的连通 k 次正则图叫作 Ramanujan图?

Ramanujan 是具有特殊才华而又英年早逝的印度数学家. 1887年12月22日他生于印度南部小镇 Erode 的外祖父家里,不久便随母亲回到距马德拉斯30公里的 Kumbakonam 镇,父亲在这里的一家衣服商店作店员. 他从10岁开始就在当地图书馆里自学数学. 1903年开始在笔记本上记录他的没有证明的数学发现,这一年高中毕业后,他以优等生的成绩考取了本镇的"政府学院",这时他完全沉醉于数学研究之中,荒废了所有其他课程. 一年后他因学习成绩不好被勒令退学. 此后直到1910年他在家自学数学和孤立地从事数学研究,写了许多笔记.

1909年他结婚后,为了挣钱养家找到一份职业,老板 S. N. Aiuar 也是一位数学爱好者,鼓励他用英文写下他的数学发现. 1913年1月16日,他把手稿寄给英国著名数学家、剑桥大学教授 Hardy. Hardy 对于他关于连分数的一些公式给予高度评价,并请他去剑桥. 不顾家庭的反对和经济上的清贫,1914年5月17日他离开印度动身去剑桥大学. 在以后的三年里,他写了许多文章,包括三篇非常重要的论文,对于后来的数论和模形式理论的发展有极大的影响. 1917年,由于生活艰苦和经常熬夜而身患重病(传说是肺结核),在医院休息两年,然后回到印度与妻子团聚. Banaras Hindu 大学马上聘他为教授,他当时没有接受,但答应待身体恢复后再去执教. 不幸他的病没有好转,1920年4月26日在他32岁的时候与世长辞.

他一生发表了37篇数学论文，保存了三个笔记本，还有许多未发表的文章和手稿. 现在有美国数学家 Audrews 和 Berndt 等人专门研究他的手稿和笔记本. 1987年，在美国伊利诺大学和印度 Tata 数学研究所，世界著名的数论学家举行学术会议，以纪念这位杰出数学家诞辰一百周年. 他的工作现在与许多数学学科（数论，代数群表示论，Kac-Moody 代数，组合数学）以及物理学发生联系. 最近十年里，有大约三百篇数学论文在题目或者摘要中提到他的名字. 他在短促的一生中提出许多数学猜想. 仅在与 Hardy 的通信中就提出一百多个没有证明的数学论断，显示了他惊人的数学直觉. 他的最著名的一个猜想是关于模形式 Fourier 展开式系数的估计. 这个著名的拉氏猜想于1973年被1978年 Fields 奖获得者 Deligne 所证明.

1988年，Lubotzky，Phillips 和 Sarnak 对于每个素数 p，构作了 $p+1$次拉氏图族. 换句话说，问题3.3.1对于 $k=p+1$答案是肯定的. 他们的办法是：考虑局部域 Q_p 上的二次线性群 $GL_2(Q_p)$对于适当同余子群的商群. 利用黎曼流形上拉普拉斯算子和它的谱理论的离散模拟，得到 $p+1$次拉氏图族. 其中证明它们的次根$\leqslant 2\sqrt{p+1-1}=2\sqrt{p}$的关键之处，正是利用了上面（已被证明）的拉氏猜想！另一方面，1990年 fields 奖获得者、苏联年青数学家 Drinfeld 在几年前曾经对于函数域的情形证明了拉氏猜想的一个类比命题. 基于这个结果，1989年 Morgenstern 对于每个素数幂 $q=p^l\geqslant 4$，构作了 $q+1$次拉氏图族. 目前，这两项结果是对于问题3.3.1的全部解答，除此之外我们一无所知. 例如对于 $k=7$，人们既没有构作出5次拉氏图族来，也没有证明出7次拉氏图族是不存在的.

正是由于上面所说的数学背景，Sarnak 等人把次根$\leqslant 2\sqrt{k-1}$的连通 k 次正则图称之为拉氏图，以显示 Ramanujan 的

数学工作(以及近年来人们在纯粹数学中取得的重大结果)对于图论和通信网络理论的新的影响.

从以上的描述可以感受到,问题3.3.1(即:能否构作 k 次拉氏图族)是相当困难的.但是,构作个别的拉氏图要相对容易.我们在下面两节将介绍用有限域构作拉氏图的一些办法.

§3.4 拉氏图的构作(一):组合方法

为了构作拉氏图,我们先作一项准备工作,设 $a_0, a_1, a_2, \cdots, a_{n-1}$ 是 n 个实数,则

$$M(a_0, a_1, \cdots, a_{n-1}) = \begin{bmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-2} & a_{n-1} \\ a_1 & a_2 & a_3 & \cdots & a_{n-1} & a_0 \\ a_2 & a_3 & a_4 & \cdots & a_0 & a_1 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n-1} & a_0 & a_1 & \cdots & a_{n-3} & a_{n-2} \end{bmatrix}$$

是 n 阶实对称方阵.我们的目的是想求出这个方阵的所有 n 个特征根,设 $w=e^{2\pi\sqrt{-1}/n}$,我们有熟知的公式(对于整数 b)

$$\sum_{a=0}^{n-1} w^{ab} = \begin{cases} n, & \text{如果 } b \text{ 是 } n \text{ 的倍数} \\ 0, & \text{否则} \end{cases} \tag{1}$$

又令

$$x_i = (1, w^i, w^{2i}, \cdots, w^{(n-1)i}) \qquad (0 \leqslant i \leqslant n-1)$$

利用(1)式可知 $x_0, x_1, \cdots, x_{n-1}$ 是两两正交的向量,再令

$$\lambda_i = \sum_{s=0}^{n-1} a_s w^{is} \qquad (0 \leqslant i \leqslant n-1)$$

则对每个整数 t,

$$\sum_{s=0}^{n-1} a_{s+t} w^{is} = \sum_{s=0}^{n-1} a_s w^{i(s-t)} = w^{-it} \lambda_i \tag{2}$$

(这里当 $m\geqslant n$ 时，规定 $a_m=a_{m-n}$)

3.4.1 定理 (A) 当 $n=2m+1$ 为奇数时，方阵 $M(a_0,a_1,\cdots,a_{n-1})$ 的 n 个特征根为

$$\lambda_0=\sum_{s=0}^{n-1}a_s \text{ 和 } \pm|\lambda_i| \quad (1\leqslant i\leqslant m).$$

(B) 当 $n=2m$ 为偶数时，方阵 $M(a_0,a_1,\cdots,a_{n-1})$ 的 n 个特征根为

$$\lambda_0=\sum_{s=0}^{n-1}a_s,\quad \lambda_m=\sum_{s=0}^{n-1}(-1)^s a_s \text{ 和} \pm|\lambda_i| \quad (1\leqslant i\leqslant m-1).$$

(注意 $\lambda_i=\bar{\lambda}_{n-i}$)

证明 (A) 设 $n=2m+1$. 考虑 n 阶方阵

$U=(x_0^T,x_1^T,x_{n-1}^T,x_2^T,x_{n-2}^T,\cdots,x_m^T,x_{n-m}^T)\quad (n-m=m+1)$

利用 $x_i(0\leqslant i\leqslant n-1)$ 彼此正交可知

$$U^TU=nI_n,$$

从而 U 是可逆方阵，再利用(2)式不难验证有

$M(a_0,\cdots,a_{n-1})U$

$$=\begin{bmatrix}\lambda_0 & \lambda_1 & \lambda_{-1} & \cdots & \lambda_m & \lambda_{-m}\\ \lambda_0 & w^{-1}\lambda_1 & w\lambda_{-1} & \cdots & w^{-m}\lambda_m & w^m\lambda_{-m}\\ \vdots & \vdots & \vdots & & \vdots & \vdots\\ \lambda_0 & w^{-(n-1)}\lambda_1 & w^{(n-1)}\lambda_{-1} & \cdots & w^{-(n-1)m}\lambda_m & w^{(n-1)m}\lambda_{-m}\end{bmatrix}$$

$$=U\begin{bmatrix}\lambda_0 & & & \\ & \boxed{\begin{matrix}0 & \lambda_{-1}\\ \lambda_1 & 0\end{matrix}} & & \\ & & \ddots & \\ & & & \boxed{\begin{matrix}0 & \lambda_{-m}\\ \lambda_m & 0\end{matrix}}\end{bmatrix}$$

由于 U 是可逆的，从而 $M(a_0,a_1,\cdots,a_{n-1})$ 相似于上式最右边那

个方阵. 由于二阶方阵

$$\begin{pmatrix} 0 & \lambda_{-i} \\ \lambda_i & 0 \end{pmatrix}$$

的特征多项式为 $x^2-\lambda_i\lambda_{-i}=0$，而 $\lambda_i=\bar{\lambda}_{-i}$，从而它的两个特征根为 $\pm\sqrt{\lambda_i\lambda_{-i}}=\pm|\lambda_i|$. 于是 $M(a_0,\cdots,a_{n-1})$ 的特征根为 λ_0 和 $\pm|\lambda_i|(1\leqslant i\leqslant m)$.

(B) 设 $n=2m$，考虑 n 阶方阵

$$U=(x_0^T,x_n^T,x_1^T,x_{n-1}^T,x_2^T,x_{n-2}^T,\cdots,x_{m-1}^T,x_{m+1}^T)$$

则仍有

$$\bar{U}^TU=nI_n,$$

从而 U 是可逆方阵. 并且

$$M(a_0,\cdots,a_{n-1})U=U\begin{bmatrix} \lambda_0 & & & & \\ & \lambda_m & & & \\ & & \begin{array}{|cc|}\hline 0 & \lambda_{-1} \\ \lambda_1 & 0 \\ \hline\end{array} & & \\ & & & \ddots & \\ & & & & \begin{array}{|cc|}\hline 0 & \lambda_{-(m-1)} \\ \lambda_{m-1} & 0 \\ \hline\end{array} \end{bmatrix}$$

于是 $M(a_0,\cdots,a_{n-1})$ 的 n 个特征根为 λ_0,λ_m 和 $\pm|\lambda_i|(1\leqslant i\leqslant m-1)$. 证毕.

现在我们采用组合方法构作拉氏图，首先利用差集合. 让我们回忆差集合的定义2.4.1：设 $d_1,\cdots,d_k$ 是 k 个整数 $(k\geqslant2)$，n 为正整数 $(n\geqslant2)$. 令

$$S=\{d_i-d_j|1\leqslant i\neq j\leqslant k\}.$$

如果对于每个 $a(1\leqslant a\leqslant n-1)$，$S$ 的 $k(k-1)$ 个数中均恰好有 λ 个模 n 同余于 a，就称 $D=\{d_1,d_2,\cdots,d_k\}$ 是一个参数为 (n,k,λ)

的差集合. 我们有

$$k(k-1)=\lambda(n-1).$$

现在设 $D=\{d_1,d_2,\cdots,d_k\}$ 是参数为 (n,k,λ) 的差集合. 我们如下构作一个图 $G(D)$：它的顶点集合为 $\mathbf{Z}/n\mathbf{Z}$，即有 n 个顶点，为模 n 的 n 个同余类，可用0,1,2,…,$n-1$表示(今后每个整数均看成是 $\mathbf{Z}/n\mathbf{Z}$ 中元素，即表示这个整数所在的模 n 同余类). 另一方面，顶点 i 和 j 有边相连，当且仅当 $i+j\in D$(即指存在某个 $l,1\leqslant l\leqslant k$，使得 $i+j\equiv d_l \pmod n$). 例如：顶点0的邻居为顶点 $d_1,d_2,\cdots,d_k$；而顶点1的邻居为顶点 $d_1-1,d_2-1,\cdots,d_k-1$ 等等，不难看出，图 $G(D)$ 的联系方阵为本节开头所引入的 n 阶方阵 $M(a_0,a_1,\cdots,a_{n-1})$，其中

$$a_i=\begin{cases}1, & \text{当 } i\in D \text{ 时}\\ 0, & \text{否则}\end{cases}$$

$G(D)$ 是具有 n 个顶点的 k 次正则图.

我们现在证明：

3.4.2 定理 对于每个差集合 D，$G(D)$ 是拉氏图.

证明 根据定理3.4.1，$M(a_0,a_1,\cdots,a_{n-1})$ 的 n 个特征根的绝对值为 $\lambda_0=\sum\limits_{i=0}^{n-1}a_i=k$ 和

$$\left|\sum_{i=0}^{n-1}a_i w^{it}\right|=\left|\sum_{j=1}^{k}w^{id_j}\right| \quad (1\leqslant i\leqslant n-1).$$

但是

$$\left|\sum_{j=1}^{k}w^{id_j}\right|^2=\left(\sum_{j=1}^{k}w^{id_j}\right)\left(\sum_{l=1}^{k}w^{-id_l}\right)$$
$$=\sum_{\substack{j,l=1\\ j=l}}^{k}w^{i(d_j-d_l)}+\sum_{\substack{j,l=1\\ j\neq l}}^{k}w^{i(d_j-d_l)}$$

右边第一个和式显然为 k,而由差集合的定义可知第二个和式为(注意$1\leqslant i\leqslant n-1$)

$$\lambda\sum_{s=1}^{n-1}w^{is}=\lambda\left(\sum_{s=0}^{n-1}w^{is}-1\right)=-\lambda.$$

于是 $$\left|\sum_{j=1}^{k}w^{id_j}\right|=\sqrt{k-\lambda}\qquad(1\leqslant i\leqslant n-1).$$

这就表明 n 个特征根除了一个为 k 之外,其余 $n-1$个的绝对值均为 $\sqrt{k-\lambda}$. 因此图 $G(D)$的次根为 $\sqrt{k-\lambda}\leqslant 2\sqrt{k-1}$. 即 $G(D)$是拉氏图.

注记 (1) 根据定理3.2.3 我们知道 $G(D)$是连通的,并且不是双份图.

(2) 这种由差集合构作的连通 k 次正则图,次根 $\sqrt{k-\lambda}$比 $2\sqrt{k-1}$要好. 但另一方面,我们却不能由此构造出 k 次拉氏图族,因为对每个固定的 $k\geqslant 2$,我们不能构作出无穷多个参数为(n,k,λ)的差集合来(由于 $k(k-1)=\lambda(n-1)$,从而 $k\geqslant\sqrt{n-1}$,于是 k 随着 n 的增大而增大).

(3) 利用有限域和其他办法,目前已构作出许多差集合系列,从而可以采用定理3.4.2构作出许多拉氏图. 进而,本书中的差集合是加法循环群 Z/nZ 上的差集合. 事实上,可以用任意有限阿贝尔群上的差集合来构作拉氏图.

我们还可以用第2.7节介绍的 m 序列来构作拉氏图,在此之前,我们先介绍有限域中的两个映射. 对于有限域 F_{q^n}的每个元素 a,令

$$T(a)=\sum_{i=0}^{n-1}a^{q^i}=a+a^q+a^{q^2}+\cdots+a^{q^{n-1}},$$

如果 $a\neq 0$,令

$$N(a)=\prod_{i=0}^{n-1}a^{q^i}=a\cdot a^q\cdot a^{q^2}\cdots a^{q^{n-1}}=a^{\frac{q^n-1}{q-1}}\neq 0,$$

由于

$$T(a)^q=(a+a^q+\cdots+a^{q^{n-2}}+a^{q^{n-1}})^q=a^q+a^{q^2}+\cdots+a^{q^{n-1}}+a$$
$$=T(a),$$

$$N(a)^q=(a\cdot a^q\cdots a^{q^{n-2}}\cdot a^{q^{n-1}})^q=a^q\cdot a^{q^2}\cdots a^{q^n}\cdot a=N(a),$$

从而 $T(a)$ 和 $N(a)$ 均属于 $\boldsymbol{F}_q$（注意 $\boldsymbol{F}_q$ 中 q 个元素恰好是方程 $x^q-x=0$ 的全部解）. 于是我们有映射

$$T:\boldsymbol{F}_{q^n}\to\boldsymbol{F}_q,$$
$$N:\boldsymbol{F}_{q^n}^*\to\boldsymbol{F}_q^*.$$

T 和 N 分别叫作从 $\boldsymbol{F}_{q^n}$ 到 $\boldsymbol{F}_q$ 的**迹映射**和**范映射**. 而 $T(a)$ 和 $N(a)$ 叫作元素 a 的**迹**和**范**. 下面是这两个映射的基本性质.

3.4.3 引理 (1) $T:\boldsymbol{F}_{q^n}\to\boldsymbol{F}_q$ 是满射. 并且对于 $\boldsymbol{F}_q$ 中每个元素 a，$\boldsymbol{F}_{q^n}$ 中恰好有 q^{n-1} 个元素 x 使得 $T(x)=a$.

(2) $N:\boldsymbol{F}_{q^n}^*\to\boldsymbol{F}_q^*$ 是满射，并且对于 $\boldsymbol{F}_q^*$ 中每个元素 a，$\boldsymbol{F}_{q^n}^*$ 中恰好有 $\frac{q^n-1}{q-1}$ 个元素 x 使得 $N(x)=a$.

(3) 对于 $x,y\in\boldsymbol{F}_{q^n}$ 和 $a\in\boldsymbol{F}_q$，则

$$T(x+y)=T(x)+T(y),\quad T(ax)=aT(x),$$
$$N(xy)=N(x)N(y).$$

证明 (1) 对于每个 $a\in\boldsymbol{F}_q$，满足 $T(x)=a$ 的元素 x 是方程

$$f(x)=x^{q^{n-1}}+x^{q^{n-2}}+\cdots+x^q+x-a=0 \qquad (*)$$

的解. 由于 $f'(x)=1\neq 0$，从而此方程有 q^{n-1} 个不同的解，对于此方程的每个解 x，我们有

$$x^{q^{n-1}}+x^{q^{n-2}}+\cdots+x^q+x=a.$$

于是(注意 $a\in \boldsymbol{F}_q$)

$$
\begin{aligned}
a = a^q &= (x^{q^{n-1}} + x^{q^{n-2}} + \cdots + x^q + x)^q \\
&= x^{q^n} + x^{q^{n-1}} + \cdots + x^q.
\end{aligned}
$$

比较上面两式可知 $x^{q^n}=x$,即 $x\in \boldsymbol{F}_{q^n}$. 从而方程(*)的所有解均属于 $\boldsymbol{F}_{q^n}$,即满足 $T(x)=a$ 的 $\boldsymbol{F}_{q^n}$中元素 x 恰好有 q^{n-1}个.

类似地可证明(2),而(3)由定义直接推得.

3.4.4 引理 设 p 为系数,$q=p^n(n\geqslant 1)$.T 是从 $\boldsymbol{F}_q$ 到 $\boldsymbol{F}_p$ 的迹映射. 则对于 $a\in \boldsymbol{F}_q$,$u=e^{2\pi\sqrt{-1}/p}$,

$$
\sum_{b\in \boldsymbol{F}_q} u^{T(ab)} = \begin{cases} 0, & 若\ a\neq 0 \\ q, & 若\ a=0. \end{cases}
$$

证明 若 $a=0$,显然

$$
\sum_{b\in \boldsymbol{F}_q} u^{T(0\cdot b)} = \sum_{b\in \boldsymbol{F}_q} u^0 = \sum_{b\in \boldsymbol{F}_q} 1 = q
$$

如果 $a\neq 0$,则当 b 过 $\boldsymbol{F}_q$ 中所有元素时,ab 也如此. 于是

$$
\sum_{b\in \boldsymbol{F}_q} u^{T(ab)} = \sum_{b\in \boldsymbol{F}_q} u^{T(b)}.
$$

根据引理3.4.3,对于 $\boldsymbol{F}_p$ 中每个元素 $c(0\leqslant c\leqslant p-1)$,$\boldsymbol{F}_q$ 中恰好有 q/p 个元素 b 使得 $T(b)=c$. 于是

$$
\sum_{b\in \boldsymbol{F}_q} u^{T(b)} = \sum_{c=0}^{p-1} \frac{q}{p} u^c = \frac{q}{p} \sum_{c=0}^{p-1} u^c = 0.
$$

证毕.

现在用第2.7节介绍的 m 序列来构作拉氏图,设 $q=p^n$,其中 p 为素数,$n\geqslant 1$. 令

$$
\underline{c} = c_0 c_1 \cdots c_{q^n-2} \cdots
$$

是 $\boldsymbol{F}_q$ 上的一个 n 级的 m 序列(周期长度为 q^n-1),于是 c_i 均为

F_q 中元素. 我们现在构作一个图 $G(\underline{c})$. 它的顶点集合为 $\{v_0, v_1, \cdots, v_{q^n-2}\}$. 而顶点 v_i 和 v_j 有边当且仅当 $c_{i+j}=1$. $G(\underline{c})$ 有 q^n-1 个顶点. 不难看出图 $G(\underline{c})$ 的联系方阵有形式 $M(a_0, a_1, \cdots, a_{q^n-2})$, 其中

$$a_i = \begin{cases} 1, & \text{若 } c_i = 1 \\ 0, & \text{否则} \end{cases}$$

由于 m 序列 $\underline{c}$ 的一个周期中共有 q^{n-1} 个1(定理2.7.2), 从而 $a_0, a_1, \cdots, a_{q^n-2}$ 中恰有 q^{n-1} 个1, 于是 $G(\underline{c})$ 为 q^{n-1} 次正则图.

3.4.5 定理 当 $n\geqslant 2$ 时, $G(\underline{c})$ 是具有 q^n-1 个顶点、q^{n-1} 次正则的拉氏图.

证明 根据定理3.4.1, 我们只需证明: 对于 $w = e^{2\pi\sqrt{-1}/(q^n-1)}$ 和 $1\leqslant i\leqslant q^n-2$,

$$\lambda_i = \sum_{s=0}^{q^n-2} a_s w^{is}$$

的绝对值均不超过 $2\sqrt{q^{n-1}-1}$. 注意

$$\lambda_i = \sum_{s=0}^{q^n-2} a_s w^{is} = \sum_{\substack{s=0 \\ c_s=1}}^{q^n-2} w^{is}$$

$$= \frac{1}{q}\sum_{s=0}^{q^n-2} w^{is} \sum_{b\in F_q} u^{T(b(c_s-1))}, \quad \text{(引理3.4.4)}$$

其中 $u=e^{2\pi\sqrt{-1}/p}$, T 是 F_q 对于 F_p 的迹映射. $b=0$ 对于上式右边的贡献为

$$\frac{1}{q}\sum_{s=0}^{q^n-2} w^{is} = 0 \qquad (\text{注意 } 1\leqslant i\leqslant q^n-2).$$

从而上式右边等于

$$\frac{1}{q}\sum_{s=0}^{q^n-2}w^{is}\sum_{b\in F_q^*}u^{T(bc_s-b)}=\frac{1}{q}\sum_{b\in F_q^*}u^{-T(b)}\sum_{s=0}^{q^n-2}u^{T(bc_s)}w^{is},$$

于是

$$|\lambda_i|^2=\frac{1}{q^2}\sum_{b,b'\in F_q^*}u^{-T(b-b')}\sum_{s,s'=0}^{q^n-2}u^{T(bc_s-b'c_{s'})}w^{i(s-s')}.$$

令 $b'=db$，$t=s-s'$，则上式右边等于

$$\frac{1}{q^2}\sum_{b,d\in F_q^*}u^{-T(b(1-d))}\sum_{s,t=0}^{q^n-2}u^{T(b(c_{s+t}-dc_s))}w^{it}$$

$$=\frac{1}{q^2}\sum_{b,d\in F_q^*}u^{-T(b(1-d))}\sum_{t=0}^{q^n-2}w^{it}\sum_{s=0}^{q^n-2}u^{T(b(c_{s+t}-dc_s))}.$$

根据第2.6和2.7节，序列 $L^t\underline{c}-d\underline{c}$ 的第 s 位恰好为 $c_{s+t}-dc_s$（其中 L 是左平移算子）. 所以 $\{(c_{s+t}-dc_s)\,|\,0\leqslant s\leqslant q^n-2\}$ 恰好是 $L^t\underline{c}-d\underline{c}$ 的一个周期. 如果 $\underline{c}\in S(f)$，其中 $f(x)$ 是 $F_q[x]$ 中 n 次本原多项式，那末 $L^t\underline{c}$，$d\underline{c}$ 和 $L_t\underline{c}-d\underline{c}$ 均属于 $S(f)$，于是存在唯一的 $t_d(0\leqslant t_d\leqslant q^n-2)$，使得 $L^{t_d}\underline{c}=d\underline{c}$. 而当 $t\neq t_d$ 时，$L^t\underline{c}-d\underline{c}$ 为 $S(f)$ 中非零序列，所以仍为 n 级 m 序列，当 $t\neq t_d$ 时，m 序列 $L^t\underline{c}-d\underline{c}$ 的一个周期 $\{(c_{s+t}-dc_s\,|\,0\leqslant s\leqslant q^n-2\}$ 中共有 $q^{n-1}-1$ 个0和 q^{n-1} 个 a（对每个 $a\in F_q^*$）. 因此当 $t\neq t_d$ 时，

$$\sum_{s=0}^{q^n-2}u^{T(b(c_{s+t}-dc_s))}=(q^{n-1}-1)+q^{n-1}\sum_{a\in F_q^*}u^{T(ba)}$$

$$=-1+q^{n-1}\sum_{a\in F_q}u^{T(ba)}=-1\qquad（引理3.4.4），$$

所以

$$\sum_{t=0}^{q^n-2}w^{it}\sum_{s=0}^{q^n-2}u^{T(b(c_{s+t}-dc_s))}=(q^n-1)w^{it_d}-\sum_{\substack{t=0\\t\neq t_d}}^{q^n-2}w^{it}$$

$$=q^n w^{it_d}-\sum_{t=0}^{q^n-2} w^{it}=q^n w^{it_d},$$

于是

$$|\lambda_i|^2=\frac{q^n}{q^2}\sum_{b,d\in F_q^*} u^{-T(b(1-d))} w^{it_d}$$

$$=q^{n-2}\sum_{d\in F_q^*} w^{it_d}\sum_{b\in F_q^*} u^{-T(b(1-d))}.$$

又根据引理3.4.4，

$$\sum_{b\in F_q^*} u^{-T(b(1-d))}=\begin{cases}-1, & \text{若 } d\neq 1.\\ q-1, & \text{若 } d=1.\end{cases}$$

于是

$$|\lambda_i|^2=q^{n-2}\Big[(q-1)w^{it_1}-\sum_{\substack{d\in F_q^*\\ d\neq 1}} w^{it_d}\Big]$$

$$=q^{n-2}\Big[qw^{it_1}-\sum_{d\in F_q^*} w^{it_d}\Big]$$

$$=q^{n-2}\Big[q-\sum_{d\in F_q^*} w^{it_d}\Big] \qquad (\text{易知 } t_1=0).$$

注意 t_d 是满足 $L^{t_d}\underline{c}=d\underline{c}$，$0\leqslant t_d\leqslant q^n-2$的唯一的整数. 现在利用定理2.6.6. 若$\underline{c}$ 对应的幂级数为$\dfrac{g(x)}{f(x)}$，则 $L^{t_d}\underline{c}$ 和 $d\underline{c}$ 对应的幂级数分别为$[x^{q^n-1-t_d}g(x)]/f(x)$和 $dg(x)/f(x)$. 从而

$$x^{q^n-1-t_d}g(x)\equiv dg(x) \quad (\mathrm{mod}\ f(x)).$$

由于 $g(x)$与 $f(x)$互素，因此

$$1\equiv x^{q^n-1}\equiv dx^{t_d} \quad (\mathrm{mod}\ f(x)).$$

由于 $d^{q-1}=1$，从而 $x^{t_d(q-1)}\equiv 1(\mathrm{mod} f(x))$. 由于 n 次本原多项式 $f(x)$的周期为 q^n-1. 从而$(q^n-1)\,|\,t_d(q-1)$，即$\dfrac{q^n-1}{q-1}\,|\,t_d$. 由于 $0\leqslant t_d\leqslant q^n-2$中满足此条件的 t_d 只有 $q-1$个，即$\dfrac{q^n-1}{q-1}t(0\leqslant t\leqslant$

$q-2$)，所以$\{t_d | d\in F_q^*\}$恰好就是这$q-1$个整数. 于是

$$\sum_{d\in F_q^*} w^{it_d} = \sum_{t=0}^{q-2} w^{it\frac{q^n-1}{q-1}}$$

$$= \sum_{t=0}^{q-2} v^{it} \quad （其中\ v = w^{\frac{q^n-1}{q-1}} = e^{2\pi\sqrt{-1}/(q-1)}）$$

$$= \begin{cases} q-1, & 若(q-1)|i,\ 1\leqslant i\leqslant q^n-2 \\ 0, & 若(q-1)\nmid i, 1\leqslant i\leqslant q^n-2. \end{cases}$$

于是$|\lambda_i|^2\leqslant q^{n-1}\leqslant 4(q^{n-1}-1)$. 即$|\lambda_i|\leqslant 2\sqrt{q^{n-1}-1}$，从而$G(\underline{c})$是拉氏图(并且由于$k=q^{n-1}$为其联系矩阵的单重特征根，而$-k$不是特征根，从而$G(\underline{c})$是连通的，并且不是双份图). 证毕.

上面我们实际上证明了q^{n-1}次正则图$G(\underline{c})$的次根为

$$\lambda(G(\underline{c})) = \begin{cases} q^{\frac{n-1}{2}}, & 当\ q\geqslant 3时, \\ 2^{\frac{n-2}{2}}, & 当\ q=2时. \end{cases}$$

根据定理3.2.5 可知当$q=2$时，

$$d(G(\underline{c}))\leqslant\left[\frac{\log(2^n-2)}{\log(2^{n-1}/2^{\frac{n-2}{2}})}\right]+1$$

$$=\left[\frac{2n\log 2+2\log(1-2^{-(n-1)})}{n\log 2}\right]+1=2,$$

从而当$n\geqslant 2, q=2$时，图$G(D)$的直径为2. 而当$n\geqslant 3, q\geqslant 3$时，

$$d(G(\underline{c}))\leqslant\left[\frac{\log(q^n-2)}{\log(q^{n-1}/q^{(n-1)/2})}\right]+1$$

$$=\left[\frac{2n\log q+2\log(1-2q^{-n})}{(n-1)\log q}\right]+1=3.$$

因此$G(\underline{c})$的直径为2或者3. 再根据图$G(D)$的定义，我们得到m序列如下的性质.

3.4.6 定理 设$\underline{c}=c_0, c_1, c_2\cdots c_{q^n-2}\cdots$是有限域$F_q$上的$n$级$m$序列. $n\geqslant 3$.

(1) 当 $q=2$ 时，对于任意两个非负整数 i 和 j，均存在整数 k，使得 $c_{i+k}=c_{k+j}=1$.

(2) 当 $q\geqslant 3$ 时，对于任意两个非负整数 i 和 j，均存在整数 k 和 l，使得 $c_{i+k}=c_{k+l}=c_{l+j}=1$.

3.4.7 习 题

1. 设 T 为有限域 F_{q^n} 对于 F_q 的迹映射，α 为 F_{q^n} 中一个本原元素. 对于 F_{q^n} 中非零元素 β，令 $c_i=T(\beta\alpha^i)$　$(i=0,1,2,\cdots)$. 求证

$$\underline{c}=c_0c_1c_2\cdots$$

是 F_q 上的 n 级 m 序列，并且 F_q 上的每个 n 级 m 序列 $\underline{c}$ 均可表示成这种形式，即 F_{q^n} 中必有某个本原元素 α 和非零元素 β，使得

$$c_i=T(\beta\alpha^i)\quad (i=0,1,2,\cdots).$$

2. 设 $n\geqslant 3$. α 为 F_{q^n} 中一个本原元素. T 表示 F_{q^n} 对于 F_q 的迹. 如果 $q=2$，则对任意两个整数 i 和 j，均存在整数 k，使得

$$T(\alpha^{i+k})=T(\alpha^{k+j})=1.$$

如果 $q\geqslant 3$，则对任意两个整数 i 和 j，以及 F_q 中任意非零元素 a，均存在整数 k 和 l，使得

$$T(\alpha^{i+k})=T(\alpha^{k+l})=T(\alpha^{l+j})=a.$$

3. 设 $n\geqslant 2$，α 为 F_{q^n} 中一个本原元素，T 表示 F_{q^n} 对于 F_q 的迹映射.

(A) 对于任意两个正整数 i 和 j，以 $N_2(i,j)$ 表示满足 $T(\alpha^{i+k})=T(\alpha^{k+j})=1$ 的整数 $k(0\leqslant k\leqslant q^n-2)$ 的个数. 则

$$N_2(i,j)=\begin{cases} q^{n-1}, & 若\ i\equiv j(\mathrm{mod}\ q^n-1) \\ 0, & 若\ i\not\equiv j(\mathrm{mod}\ q^n-1),i\equiv j(\mathrm{mod}\ \dfrac{q^n-1}{q-1}) \\ q^{n-2}, & 若\ i\not\equiv j(\mathrm{mod}\ \dfrac{q^n-1}{q-1}). \end{cases}$$

(B) 以 $N_3(i,j)$ 表示满足 $T(\alpha^{i+k})=T(\alpha^{k+l})=T(\alpha^{l+j})=1$ 的整数对 $(k,l)(0\leqslant k,l\leqslant q^n-2)$ 的个数. 求证

$$N_3(i,j)=\begin{cases}q^{2n-3}+q^{n-1}-q^{n-2}, & 若\ T(\alpha^{i+j})=1\\ q^{2n-3}, & 若\ T(\alpha^{i+j})=0\\ q^{2n-3}-q^{n-2}, & 若\ T(\alpha^{i+j})\neq 1,0\end{cases}$$

(C)由 F_q 上 n 级 m 序列 $\underline{c}$ 构作的图 $G(\underline{c})$ 的直径为

$$d(G(\underline{c}))=\begin{cases}2, & 若\ q=2\\ 3, & 若\ q\geqslant 3.\end{cases}$$

4. 设 $n\geqslant 3$，求证 n 个顶点的连通2次正则图 C_n 必为拉氏图(所以问题3.3.1对于 $k=2$ 答案是肯定的)，其中 C_n 如图6所示.

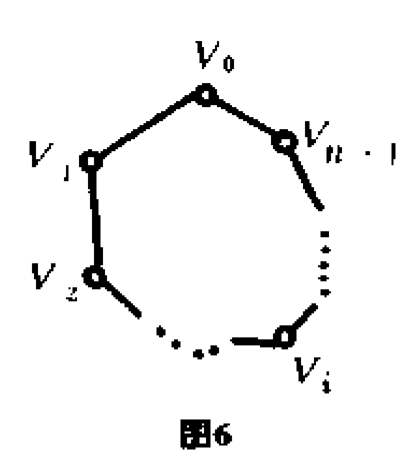


图6

§3.5 拉氏图的构作(二)：有限域方法

上节中我们利用差集合与 m 序列的组合特性构作了一系列拉氏图，其中也利用了有限域的知识. 本节中我们进一步应用有限域的结构来构作拉氏图.

设 p 为素数，整数 $c\geqslant 2$，并且 $c\mid(p-1)$. 令 $p-1=ck$，并且设 $k\geqslant 2$. 以 g 表示有限域 F_p 的一个本原元素，即 g 是模 p 的原根. 则 $F_p^*=\{g^0=1,g,g^2,\cdots,g^{p-2}\}$. 令

$$S=\{g^0=1,g^c,g^{2c},\cdots,g^{(k-1)c}\}$$

则 S 中 k 个元素恰好是 F_p^* 中可以表成 c 次幂的那些元素. 令

$$a_i=\begin{cases}1, & 若\ i\in S\\ 0, & 否则.\end{cases}$$

以 $G(p,c)$ 表示联系方阵为 $M(a_0,a_1,\cdots,a_{p-1})$ 的图. 这是具有 p 个顶点的 k 次正则图. 如果以 $v_0,v_1,\cdots,v_{p-1}$ 表示图中 p 个顶点，则图中顶点 v_i 和 v_j 之间有边的充分必要条件为 $i+j\in S$. 我们

现在估计图 $G(p,c)$ 的次根，即估计方阵 $M(a_0,\cdots,a_{p-1})$ 中除了大根 k 之外的其余特征根.

根据定理3.4.1，方阵 $M(a_0,\cdots,a_{p-1})$ 的所有特征根可表为（令 $w=e^{2\pi\sqrt{-1}/p}$）

$$\lambda_0=\sum_{s=0}^{p-1}a_s=k \quad \text{和} \quad \lambda_i=\pm\left|\sum_{s=0}^{p-1}a_s w^{is}\right| \left(1\leqslant i\leqslant\frac{p-1}{2}\right).$$

为了估计 $\lambda_i(1\leqslant i\leqslant p-1)$，我们定义如下的映射

$$\varphi: \boldsymbol{F}_p^* \longrightarrow \boldsymbol{Z}/(p-1)\boldsymbol{Z},$$

$$s \longmapsto \varphi(s)=l,$$

其中 l 是由 $s\equiv g^l(\mathrm{mod}\ p)$ 决定的整数. 由于 g 的阶为 $p-1$，满足 $s\equiv g^l(\mathrm{mod}\ p)$ 的不同整数 l 彼此相差 $(p-1)$ 的倍数，从而 l 作为 $\boldsymbol{Z}/(p-1)\boldsymbol{Z}$ 中的元素是唯一确定的. φ 是集合 $\boldsymbol{F}_p^*$ 与 $\boldsymbol{Z}/(p-1)\boldsymbol{Z}$ 之间的一一对应，并且有如下性质：

$$\varphi(ss')=\varphi(s)+\varphi(s'), \quad \varphi(s^{-1})=-\varphi(s), \quad \varphi(1)=0.$$

不难看出，$\boldsymbol{F}_p^*$ 中元素 s 属于集合 S 的充分必要条件是 $c|\varphi(s)$. 令 $u=e^{2\pi\sqrt{-1}/c}$. 由于

$$\sum_{j=0}^{c-1}u^{ij}=\begin{cases}0, & \text{若 } c\nmid i\\ c, & \text{若 } c|i\end{cases}.$$

从而对每个 $s\in\boldsymbol{F}_p^*$，

$$\sum_{j=0}^{c-1}u^{j\varphi(s)}=\begin{cases}0, & \text{若 } s\notin S\\ c, & \text{若 } s\in S.\end{cases}$$

于是

$$\sum_{s=0}^{p-1}a_s w^{is}=\sum_{\substack{s=1\\ s\in S}}^{p-1}w^{is}=\frac{1}{c}\sum_{s=1}^{p-1}w^{is}\sum_{j=0}^{c-1}u^{j\varphi(s)}$$

$$=\frac{1}{c}\sum_{j=0}^{c-1}\sum_{s=1}^{p-1}w^{is}u^{j\varphi(s)}=\frac{1}{c}\sum_{j=0}^{c-1}G(j),$$

其中 $G(j)=\sum_{s=1}^{p-1}w^{is}u^{j\varphi(s)}$ 通常叫作有限域 F_p 上的**高斯和**. 当 $j=0$ 时,

$$G(0)=\sum_{s=1}^{p-1}w^{is}=\sum_{s=0}^{p-1}w^{is}-1=-1.$$

而当 $1\leqslant j\leqslant c-1$ 时,

$$|G(j)|^2=\sum_{s,s'=1}^{p-1}w^{i(s-s')}u^{j(\varphi(s)-\varphi(s'))}$$
$$=\sum_{s,s'=1}^{p-1}w^{i(s-s')}u^{j\varphi(s/s')}.$$

令 $s=s't$,则

$$|G(j)|^2=\sum_{s',t=1}^{p-1}w^{is'(t-1)}u^{j\varphi(t)}$$
$$=\sum_{t=1}^{p-1}u^{j\varphi(t)}\sum_{s'=1}^{p-1}w^{is'(t-1)}$$
$$=u^{j\varphi(1)}(p-1)+\sum_{t=2}^{p-1}u^{j\varphi(t)}(-1)$$
$$=p-\sum_{t=1}^{p-1}u^{j\varphi(t)}\quad(\text{由于 }\varphi(1)=0)$$
$$=p-\sum_{l=0}^{p-2}u^{jl}\quad(\text{由于 }\varphi\text{ 是一一对应})$$
$$=p\qquad(\text{由于 }1\leqslant j\leqslant c-1).$$

因此

$$|G(j)|\leqslant\sqrt{p}\quad(1\leqslant j\leqslant c-1).$$

$$|\lambda_i|=\frac{1}{c}\left|\sum_{j=0}^{c-1}G(j)\right|\leqslant\frac{1}{c}\sum_{j=0}^{c-1}|G(j)|$$
$$=\frac{1}{c}(1+(c-1)\sqrt{p}).\qquad\left(1\leqslant i\leqslant\frac{p-1}{2}\right).$$

于是图 $G(p,c)$ 的次根 $\leqslant\frac{1}{c}(1+(c-1)\sqrt{p})$. 由于 $G(p,c)$ 是 k

$=\frac{p-1}{c}$次正则图. 所以当

$$\frac{1}{c}(1+(c-1)\sqrt{p})\leqslant 2\sqrt{\frac{p-1}{c}-1} \qquad (*)$$

时, $G(p,c)$为拉氏图. 当 p 充分大时, 这个不等式的左边和右边的主要部份分别为$\frac{c-1}{c}\sqrt{p}$和$2\sqrt{\frac{p}{c}}$. 所以当$\frac{c-1}{c}<2\sqrt{\frac{1}{c}}$时, 即$1\leqslant c\leqslant 5$时, 对于充分大的素数 p, $(*)$式成立. 根据数论中一个著名的定理. 对每个正整数 c, 满足 $c|(p-1)$的素数 p 有无穷多个. 所以对于每个 c, $1\leqslant c\leqslant 5$, 我们构作出无穷多个拉氏图 $G(p,c)$.

综合上述, 我们证明了:

3.5.1 定理 设 c 是整数, $1\leqslant c\leqslant 5$. p 为素数, 并且 $p-1=ck$, 其中 k 为整数, $k\geqslant 2$, 则当

$$\frac{1}{c}(1+(c-1)\sqrt{p})\leqslant 2\sqrt{\frac{p-1}{c}-1} \qquad (*)$$

时, p 个顶点的$\frac{p-1}{c}$次正则图 $G(p,c)$是拉氏图.

注记 我们在证明中利用了高斯和的估计$|G(j)|=\sqrt{p}$ $(1\leqslant j\leqslant c-1)$. 事实上, 可以对高斯和 $G(j)$的值作更精确的计算, 从而能够去掉定理中的不等式条件$(*)$, 并且还可允许 $c=6$. 即可以证明对每个$1\leqslant c\leqslant 6$, 和素数 $p(p-1=ck, k\geqslant 2)$, $G(p,c)$均是拉氏图.

注记 以上我们是利用有限域 F_p 构作出拉氏图, 对于每个素数幂 q, 利用有限域 F_q 和 F_q 上的高斯和计算, 我们可以构作出具有 q 个顶点的$\frac{q-1}{c}$次正则拉氏图, 其中$1\leqslant c\leqslant 6$, 而$\frac{q-1}{c}$是$\geqslant 2$的整数.

近年来，人们利用有限域构作了许多拉氏图，在估计这些图的次根时，采用了有限域上各种特征和的估计，这些估计本质上均基于关于代数曲线在有限域中解数的著名的 Weil 定理. 在这本小册子中我们无法介绍关于有限域的这些深刻的理论. 所以下面我们只介绍结果而略去证明.

3.5.2 （金芳蓉，1989） 设 $t\geqslant 2$. g 为有限域 F_{q^t} 中一个本原元素，w 是 F_{q^t} 中一个元素，使得 $F_{q^t}=F_q(w)$，即 w 是 $F_q[x]$ 中一个 t 次不可约方程的根. 设 F_q 中 q 个元素为 $c_1,c_2,\cdots,c_q$，又设

$$w+c_i=g^{d_i}\qquad(1\leqslant i\leqslant q),$$

其中整数 d_i 看作 $Z/(q^t-1)Z$ 中的元素是唯一确定的. 于是我们得到 $Z/(q^t-1)Z$ 中的 q 元子集

$$S=\{d_1,d_2,\cdots,d_q\}.$$

现在我们构作一个具有 q^t-1 个顶点的 q 次正则图 $K(q,t)$，它的顶点是 $v_0,v_1,\cdots,v_{q^t-2}$. 而顶点 v_i 和 v_j 有边的充分必要条件是 $i+j\in S$. 我们知道，图 $K(q,t)$ 的联系方阵为 $M(a_0,a_1,\cdots,a_{q^t-2})$，其中

$$a_i=\begin{cases}1, & 若\ i\in S\\ 0, & 否则\end{cases}.$$

并且这个方阵的所有特征根的绝对值为 k 和

$$\left|\sum_{i=1}^{q}w^{jd_i}\right|\quad(1\leqslant j\leqslant q^t-2),\quad w=e^{2\pi\sqrt{-1}/(q^t-1)}.$$

利用 N. Katz（普林斯顿大学著名数论学家）对于特征和的一个估计，可以证明上述绝对值均小于等于 $(t-1)\sqrt{q}$. 特别当 $t=2$ 时，$K(q,2)$ 是拉氏图（具有 q^2-1 个顶点的 q 次正则图，次根小于等于 $\sqrt{q}$）.

3.5.3 （李文卿，1990） 以 N 表示 $\boldsymbol{F}_{q^n}$ 对于 $\boldsymbol{F}_q$ 的范映射，$N_n=\{x\in \boldsymbol{F}_{q^n}^* \mid N(x)=1\}$，则 N_n 共有 $(q^n-1)/(q-1)$ 个元素（引理 3.4.3）. 设 $\{c_0,c_1,\cdots,c_{q^n-1}\}$ 为 $\boldsymbol{F}_{q^n}$ 中 q^n 个元素，现在构作图 $X(q^n)$：它的顶点为 $\{v_0,v_1,\cdots,v_{q^n-1}\}$，顶点 v_i 和 v_j 有边的充分必要条件是 $c_i+c_j\in N_n$. 易知这是具有 q^n 个顶点的 $(q^n-1)/(q-1)$ 次正则图. 它的联系方阵是与加法群 $\boldsymbol{F}_{q^n}$ 有关的一个方阵. 利用 Delinge 给出的一个特征和的估计，可以证明图 $X(q^n)$ 的次根小于等于 $n\sqrt{q^n-1}$. 特别当 $n=2$ 时，$X(q^2)$ 是拉氏图.

3.5.4 （李文卿，1990） 设 N 是 $\boldsymbol{F}_{q^2}$ 对于 $\boldsymbol{F}_q$ 的范映射，$N_2=\{x\in \boldsymbol{F}_{q^2}^* \mid N(x)=1\}$，定义

$$N_2\times \boldsymbol{F}_{q^2}=\{(a,b)\mid a\in N_2,b\in \boldsymbol{F}_{q^2}\},$$

则 $N_2\times \boldsymbol{F}_{q^2}$ 共有 $q^2(q+1)$ 个元素，设它们为 $c_1,c_2,\cdots,c_n$，$n=q^2(q+1)$. 现在构作图 $L'(q^2)$：它的顶点全体为 $v_1,\cdots,v_n$. 而顶点 v_i 和 v_j 之间有边的充分必要条件为 $a_1a_2=b_1b_2$，其中 $c_i=(a_1,b_1)$，$c_j=(a_2,b_2)$. 图 $L'(q^2)$ 具有 $q^2(q+1)$ 个顶点并且是 $(q+1)$ 次正则图. 利用 Weil 定理可以证明这个图的次根 $\leqslant 2\sqrt{q}$，从而是拉氏图.

类似方法还可作出具有 $(q+1)(q^2-1)$ 个顶点的 $(q+1)$ 次正则拉氏图（q 为素数幂）.

3.5.5 （李文卿，1990） 设 $n\geqslant 2$，N 是 $\boldsymbol{F}_{q^n}$ 对于 $\boldsymbol{F}_q$ 的范映射，$N_n=\{x\in \boldsymbol{F}_{q^n}^* \mid N(x)=1\}$. 令 $t\in \boldsymbol{F}_{q^n}$ 使得 $\boldsymbol{F}_{q^n}=\boldsymbol{F}_q(t)$. 令 $S=\{1\}\cup\{(t^q+a)/(t+a)\mid a\in \boldsymbol{F}_q\}$，易知 S 中共有 $q+1$ 个元素，并且 S 为 N_n 的子集合. 设 N_n 中全部元素为 $c_1,c_2,\cdots,c_r$，$r=(q^n-1)/$

$(q-1)$. 现在构作图 $L''(q^n)$：它的顶点为 $v_1, v_2, \cdots, v_r$. 而 v_i 和 v_j 有边的充分必要条件为 $c_i c_j \in S$. 这是具有 $(q^n-1)/(q-1)$ 个顶点的 $(q+1)$ 次正则图. 利用 Weil 定理可以证明图 $L''(q^n)$ 的次根 $\leqslant (n-2)\sqrt{q}$. 所以 $L''(q^3)$ 和 $L''(q^4)$ 是拉氏图.

以上是近年来利用有限域构作出的一些拉氏图. 但是任何一种方法都没有构作出新的 k 次拉氏图族来. 目前的一个普遍看法是：为了构作拉氏图族，不能只用有限域的加法结构和乘法结构，甚至用交换群也是不行的，需要采用适当的非交换群和它的表示理论. 这就为研究群表示论的人们开辟了一个新的研究课题.

3.5.6 习 题

设 c 为正整数，$c \geqslant 2$，p 为素数并且 $c \mid (p-1)$，$\frac{p-1}{c} \geqslant 2$. $G(p,c)$ 是本节定义的具有 p 个顶点的 $\frac{p-1}{c}$ 次正则图. 求证

(1) 当 p 充分大时，$G(p,c)$ 的直径 $\leqslant 3$.

(2) 当 p 充分大时，对于任意正整数 i 和 j，均存在正整数 k 和 l，使得 $i+k, k+l$ 和 $l+j$ 均是 F_p^* 中元素的 c 次幂.

附 录

有没有10阶有限射影平面？

萧文强 （香港大学数学系）

1. 宴客问题

有本介绍趣味数学的经典之作，名叫《数学游戏与小品》，是波尔(W. W. ROUSE BALL)在1892年的著述. 这本饶有趣味的书问世后，出了很多个版本，里面陆续增添了一些别的名家手笔. 第10章是以这样一个问题开首的：

一位好客的女主人打算邀请她的七位朋友来家里晚宴，每晚她只能招待三位宾客，但她希望任何两位朋友都恰好在一次晚宴上见面，她应该怎样安排呢？

请读者先尝试安排，不久你便会发现任何两晚的宾客中必须有一位相同. 换句话说，如果第一晚她邀请 A、B、C，第二晚她邀请 D、E、F，这样下去肯定安排不成. 一个安排方案是这样的：

第一晚邀请 A、B、C；第二晚邀请 A、D、E；

第三晚邀请 A、F、G；第四晚邀请 B、D、F；

第五晚邀请 B、E、G；第六晚邀请 C、D、G；

第七晚邀请 C、E、F.

我们也可以用一个图表示这个方案(见图7)，图中有七点，每点表示一位女主人的朋友；若干个点组成的集合叫做线，有七条线，每条线由三点组成，即是那些在同一晚被邀请的宾客. 这个图颇有名堂，可以说是组合数学上风头最劲的图形了！由于数学家范诺(G. FANO)在1892年提出这个图形，今天我们称它作范诺构形(FANO CONFIGURATION)，它的正式“学名”可是PG(2,2)，即是定义在二元域上的二维射影几何，是一种有限射影平面. 有限射影平面是这篇文章的主角，我们要探讨的问题是有没有某种有限射影平面？如果沿用宴客问题的语言，女主人打算邀请一百一十一位朋友来家里晚宴，每晚只能招待十一位宾客，但又要求任何两位朋友都恰好在一次晚宴上见面，她应该怎样安排呢？一个安排方案是个叫做10阶有限射影平面的东西. 1988年12月20日《纽约时报》(NEW YORK TIMES)刊载了一则新闻，报导加拿大康哥迪亚大学(CONCORDIA UNIVERSITY)林永康(CLEMENT LAM)教授带领一个研究小组，运用电脑验算获至充分证据，认定不存在一个10阶有限射影平面，也就是说，上述的问题是解决不了的. 读者会问：“数学家只晓得请客吃饭吗？为什么对这个问题产生兴趣？什么叫做有限射影平面？它跟哪些

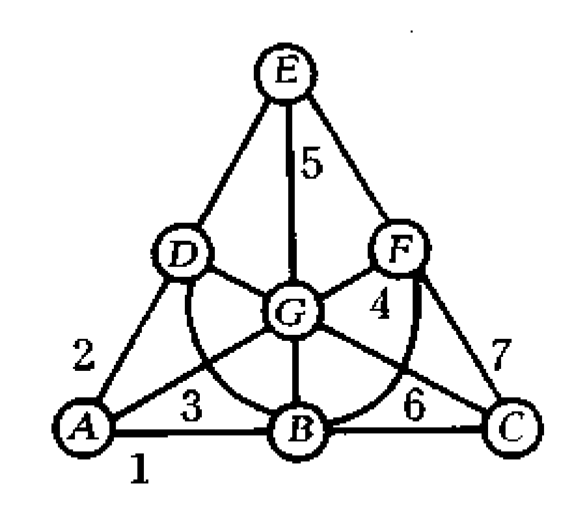


图7

数学扯上关系?"请读者稍安毋躁,听我慢慢道来.

2. 射影几何和有限射影平面

射影几何的研究,始自法国数学家笛沙格(G. DESARGUES)在1639年的著作,但这些工作在当时并没有得到重视,没有引起什么反响.直至再过了几乎两个世纪后,另一位法国数学家彭赛列(J. V. PONCELET)深受教师蒙日(G. MONGE)和卡诺(L. N. M. CARNOT)的影响,在1822年发表了他的射影几何学说,射影几何才备受数学界重视,更成为19世纪的几何研究重点.

那个时候的射影几何建基于欧氏空间的几何,让我试以欧氏平面为例作解释,如果读者对当中一些术语感到陌生的话,大可跳过这一段解释续看下去.为了不让平行线享有与众不同的特殊地位(不平行的直线延长必相交,平行的直线不论怎样延长都不相交),我们对平面补添一些"理想点".对每一组平行线我们补添一点,不妨视作这些平行线的公共相交点;全部"理想点"组成一条"理想线",于是原来的平面变成一个射影平面,里面任何两线相交于唯一的一个点,任何两点决定唯一的一条线.如果采用坐标几何的惯用手法,我们应该怎样描述这些补添的点和线呢?考虑通过原点的一条直线,在这条直线上取一点,设为(x,y),$(x/\frac{1}{2},y/\frac{1}{2})$是直线上距原点更远的一点,$(x/\frac{1}{3},y/\frac{1}{3})$是直线上距原点又更远的一点,……;这样沿着直线一直走,便会越走越接近那个"理想点"了.所以,"理想点"的坐标有些象$(x/0,y/0)$,但用0除x和y,那怎么行呢?一个转弯抹角的说法

是用$(x,y,0)$表示那一点，把0写在最后的位置，只在于表示意图而非实施用0除 x 和 y. 为求一致，我们索性把全部点都写成(x,y,z)，不过大家需要先约好，当 $z\neq 0$时，这个点其实是$(x/z, y/z)$；换句话说，所有(kx,ky,kz)，$k\neq 0$，必须给视作相同的点. 数学上有个叫做等价关系(EQUIVALENCE RELATION)和等价类(EQUIVALENCE CLASS)的概念，正是为了描述这种情况而设的. 懂得等价关系的读者便晓得刚才的叙述可以精确地写作$(\boldsymbol{R}^3\setminus\{0\})/\sim$，对三维实向量 α 和 β 来说，$\alpha\sim\beta$(α 等价于 β)表示有非零实数 k 使 $\alpha=k\beta$. 这样得来的等价类集记作 $PG(2,\boldsymbol{R})$，叫做一个二维实射影几何，或称作一个实射影平面. 更一般地，$\boldsymbol{R}$ 可给换成一个任意域 F(不懂得什么是域的读者可以把它看作是一个里面能进行四则运算的集合)，3可给换成 $n+1$，得到的等价类记作 $PG(n,F)$，叫做域 F 上的 n 维射影几何(n—DIMENSIONAL PROJECTIVE GEOMETRY).

20世纪初，经过帕施(M. PASCH)、克莱茵(F. KLEIN)、维布伦(VEBLEN)、希尔伯特(D. HILBERT)诸人的努力，通过建立射影几何的公理系统，射影几何才摆脱对欧氏空间的依赖而获至它的独立生存的权利. 让我只依射影平面(即是 $n=2$)为例作叙述，一个射影平面(PROJECTIVE PLANE)是由两个集和它们之间的一个关联关系(INCIDENCE RELATION)构成：$\mathscr{P}$ 的元叫做点(POINT)，$\mathscr{L}$ 的元叫做线(LINE)；如果 p 是 $\mathscr{P}$ 的元，l 是 $\mathscr{L}$ 的元，$P\circ l$ 表示关联. 为简化以下的叙述，我们说 p 在 l 上或 l 在 p 上；$p\circ l$ 必须满足下面四条公理：

〔$P1$〕 对 $\mathscr{P}$ 中不相同的元 P 和 Q，有且仅有一个 $\mathscr{L}$ 中元 l 使 $P\circ l$ 和 $Q\circ l$；

〔$P2$〕 对 $\mathscr{L}$ 中不相同的元 l 和 m，有且仅有一个 $\mathscr{P}$ 中元 p 使 $p\circ l$ 和 $p\circ m$；

〔P3〕 有四点，其中任何三点不在一线上；

〔P4〕 有四线，其中任何三线不经过同一点.

固然，还有别的形式的公理系统是描述同一回事，但上面的公理系统有个“自对偶”的优点，从中推导出来的每一条定理，只要把命题中的点和线的地位互易，便又是另一条定理，可谓事半功倍！读者只要回顾一下补添了“理想点”和“理想线”的平面，便自然看得出〔P1〕到〔P4〕这四条公理的几何意义了.

当 $\mathscr{P}$ 和 $\mathscr{L}$ 都是有限集时，那个射影平面叫做有限射影平面，首先由德国数学家施陶特(K. G. C. VON STAUDT)在1856年提出讨论. 范诺提出的构形，是最小的有限射影平面，有7点和7线. 它其实是二元域 $F=\{0,1\}$ 上的二维射影几何. 简记作PG(2. 2). $\mathscr{P}$ 的7点是(见图7)：

〔0,0,1〕= C 〔0,1,0〕= A 〔0,1,1〕= B 〔1,0,0〕= E

〔1,0,1〕= F 〔1,1,0〕= D 〔1,1,1〕= G；

$\mathscr{L}$ 的7线是(见图7)：

⟨0,0,1⟩=ADE， ⟨0,1,0⟩=CEF， ⟨0,1,1⟩=BEG，

⟨1,0,0⟩=ABC， ⟨1,0,1⟩=AFG， ⟨1,1,0⟩=CDG，

⟨1,1,1⟩=BDF；

而〔x,y,z〕∘⟨x',y',z'⟩当且仅当 $x'x+y'y+z'z=0$. 这个射影平面的关联关系可以利用关联表展示(见图8)，行是线，列是点. 举一个例，标以3那一行和标以 F 那一列相交的格子涂上黑色，表示点 F 在线3(即 AFG)；标以6那一行和标以 B 那一列相交的格子涂上

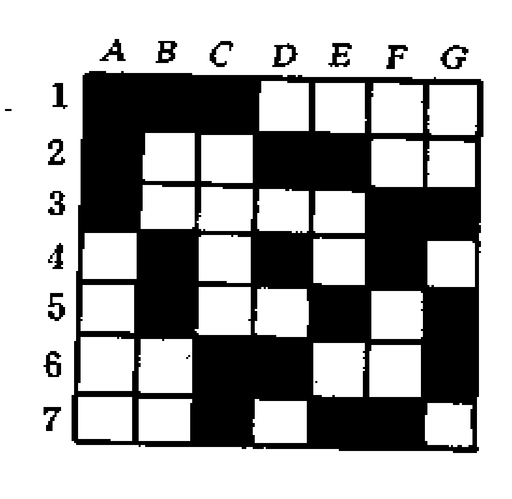


图8

白色，表示点 B 不在线6(即 CDG). 如果把黑色的格子换作1，白色的格子换作0，得到的矩阵叫做那一个射影平面的关联矩阵(INCIDENCE MATRIX)，在第3节里将大派用场. 注意，〔P1〕和〔P2〕等于说任何两列(或两行)有且仅有一个同等位置的格子是涂上黑色. 对一般有限射影平面的关联表，这个性质当然也是具备的，但眼下这一个关联表还有一个单凭肉眼不易发觉的性质，就是适当地调换行和列后，关联表的样子很特别，每一行是上一行向右边移一格得来(见图9). 要解释这个现象，需要借助有限域的知识(参阅本书正文). 这个漂亮的性质最先是由美国数学家辛格(J. SINGER)在1938年发现的. 读者自然会提出疑问："是不是任何一个有限射影平面的关联表都具备这个漂亮的性质呢?"答案是否定的，但最小的反例已经是一个91行91列的表，在本节结尾我们将要回到这一点.

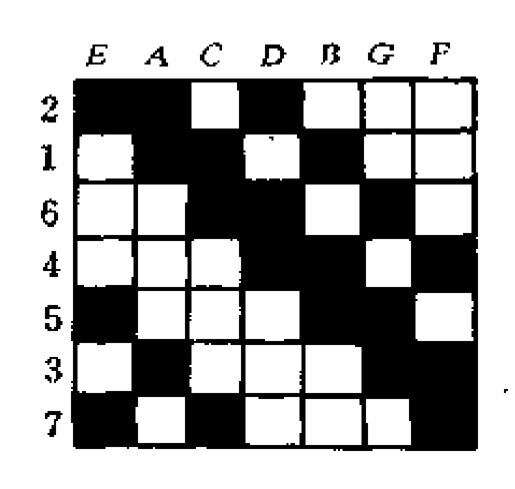


图9

读者是否也注意到关联表的每一行每一列都有同样多涂了黑色的格子呢?对一般有限射影平面的关联表，这仍然是对的. 从公理〔P1〕至〔P4〕我们能推断以下的结果：

定理1 设 N 是大于1的整数，在有限射影平面内，下列各命题互相等价：

(1) 有一线在 $N+1$点上，

(2) 有一点在 $N+1$线上，

(3) 任何线在 $N+1$点上，

(4) 任何点在 $N+1$线上，

(5) 共有 N^2+N+1个点，

(6) 共有 N^2+N+1条线.

满足这些(等价)条件的有限射影平面叫做 N 阶射影平面(PROJECTIVE PLANE OF ORDER N).

在过去一个世纪中，虽经众多数学家的努力，我们仍然摸不透有限射影平面的存在与否这个问题. 固然，对某些 N 我们肯定存在一个 N 阶射影平面，例如当 F 是个 q 元域时，$PG(2,F)=PG(2,q)$是一个 q 阶射影平面(熟悉有限域和向量空间的读者可试证明任何线上有 $q+1$个点)，由于 q 元域存在的充要条件是 q 为质数幂，我们得到下面的结果：

定理2 若 N 是个质数幂，则存在 N 阶射影平面.

通过 $PG(2,q)$构作得来的射影平面，叫做笛沙格平面，当质数幂 N 不大于8时，只有这一种射影平面，但当质数幂 N 大于8时，却存在别的射影平面. 特别地，当 N 是$9=3^2$时，很多年前数学家已经构作了几个不是笛沙格平面的9阶射影平面，它有91个点和91条线，由于并不是通过 $PG(2,9)$构作得来，它的关联表并不具备辛格发现的性质. 两年前，林永康和他的研究小组更进一步证明了只有四种不同的9阶射影平面.

3. 不存在哪些阶的射影平面?

读者在上一节见过存在 N 阶射影平面的数值 N，自然要问："有没有哪些 N 肯定不存在 N 阶射影平面呢?"至今为止，这方面的答案只有一个，就是美国数学家布鲁克(R. H. BRUCK)的赖瑟(J. H. RYSER)在1949年发现的重要结果.

定理3 (布鲁克—赖瑟) 若 N 形如$4m+1$或$4m+2$且不

能给写作两个平方数的和，则不存在 N 阶射影平面.

我不在这里证明这条重要定理，但却通过解释一个特殊情况展示证明的中心思想，当中必须假定读者具备一些对称矩阵和二次型(QUADRATIC FORM)的基本知识，不熟悉这些知识的读者跳过这段解释也无妨. 我希望说服读者，为什么不存在6阶射影平面. 如果有一个6阶射影平面，它的关联矩阵 A 是个43×43矩阵，元是0或1，射影平面的界定性质等于说 $AA^T=6I+J$，这里的 A^T 是 A 的转置矩阵、I 是单位矩阵、J 是全部元为1的矩阵. 从直接计算可知 AA^T 的行列式是 $49\times 6^{42}\neq 0$，所以 A 是非奇异矩阵. 置 $B=\begin{bmatrix} A & 0 \\ 0 & 1 \end{bmatrix}$，$B$ 是个44×44非奇异矩阵，且 $BB^T=\begin{bmatrix} 6I+J & 0 \\ 0 & 1 \end{bmatrix}$. 再置 $K=\begin{bmatrix} H & & 0 \\ & \ddots & \\ 0 & & H \end{bmatrix}$，对角线上共有11个4×4矩阵 H，$H=\begin{bmatrix} 2 & 1 & 1 & 0 \\ 1 & 2 & 0 & -1 \\ 1 & 0 & -2 & 1 \\ 0 & 1 & -1 & -2 \end{bmatrix}$. 注意到 $HH^T=6I$（这是因为 $6=2^2+1^2+1^2+0^2$），便知道 H 是非奇异矩阵. 所以 K 是个44×44非奇异矩阵，且 $KK^T=6I$. 因此，有

$(KB^{-1})\begin{bmatrix} 6I+J & 0 \\ 0 & 1 \end{bmatrix}(KB^{-1})^T=6I$，即是说下面 的两个有理数域上的二次型是相合(CONGRUENT)的：

$$(x_1+\cdots+x_{43})^2+x_{44}^2+6(x_1^2+\cdots+x_{43}^2)\text{和}$$
$$6(x_1^2+\cdots+x_{43}^2)+6x_{44}^2.$$

把未定元再作适当的变换，更可以化为下面两个有理数域上的相合二次型：

$$(x_1+\cdots+x_{43})^2+x_{44}^2\text{和}6x_{44}^2.$$

因此，存在有理数 a、b、c 满足 $a^2+b^2=6c^2$. 消去分母后，还可以设 a、b、c 是整数，由此可以推断6能被写作两个平方数的和，但这是不可能的！

让我们把从2开始的整数 N 分成三类：（Ⅰ）是质数幂；（Ⅱ）是布鲁克—赖瑟定理排除的；（Ⅲ）是其余.

（Ⅰ）	2	3	4	5		7	8	9		11		13			16	17		19		
（Ⅱ）					6								14							21
（Ⅲ）									10		12			15			18		20	

对（Ⅰ）我们知道存在 N 阶射影平面，对（Ⅱ）我们知道不存在 N 阶射影平面，对（Ⅲ）我们不肯定存在 N 阶射影平面也不肯定不存在 N 阶射影平面. 不过数学家倾向相信只有两种可能：一是当且仅当 N 在（Ⅰ）时，存在 N 阶射影平面；另一是当且仅当 N 在（Ⅰ）或（Ⅲ）时，存在 N 阶射影平面. 为了决定哪一个可能较象样，0阶射影平面存在与否，起了关键作用. 第一节结尾提到的发现，使数学家更加相信前一个猜想：N 阶射影平面存在的充要条件是 N 为质数幂.

4. 有限射影平面与某些组合数学对象的关联

让我们回到那个2阶射影平面（或称范诺构形）的关联表（见图9），把列顺次改标作0、1、2、3、4、5、6. 第一行涂上黑色的格子是0、1、3，把 $D=\{0,1,3\}$ 看作是模7同余类集合 Z_7 的子集，它有什么性质呢？由于任何一行都是第一行向右移若干格得来，而且（除第一行自身不计）它跟第一行有且仅有一个同等位置的格子

是涂上黑色，翻译成 Z_7 内的语言就是说：对任何 $t\neq 0, d_i-d_j=t$ 有唯一个有序偶 (d_i, d_j) 为解，d_i 和 d_j 是 D 中元. 说得更明白一点，D 中全部不相同元的差（模7）正好是1、2、3、4、5、6. 更一般地，如果 $D=\{d_1,\cdots,d_k\}$ 是 Z_v 的子集，且对任何 $t\neq 0, d_i-d_j=t$ 恰好有 λ 个有序偶 (d_i, d_j) 为解，d_i 和 d_j 是 D 中元，我们便说 D 是个 (v,k,λ) 一循环差集(CYCLIC DIFFERENCE SET). 这里的 $N=k-\lambda$ 是个很有意义的参数，叫做循环差集的阶. 当 $N=0$ 或1时，循环差集只能是显而易见的几种，即是空集 $\varnothing$、全集 Z_v、单元集 $\{d\}$ 或者只欠单元的余集 $Z_v\backslash\{d\}$. 当 $N\geqslant 2$ 时，可以证明 v 只在 $4N-1$ 和 N^2+N+1 中间取值. 上界值和下界值都很有意思，很多时候可以达致. 对上界值 N^2+N+1 来说，由 N 阶笛沙格射影平面 PG$(2,N)$ 得到的 $(N^2+N+1, N+1, 1)$ 一循环差集即是一个例子. 我们习惯把具有这些参数的循环差集叫做平面差集，奇怪的是迄今为止我们仍未找到不是通过 PG$(2,N)$ 得到的平面差集. 对下界值 $4N-1$ 来说，很多时候可以构作 $(4N-1, 2N-1, N-1)$ 一循环差集，我们习惯把具有这些参数的循环差集叫做阿达玛差集，刚才的 $(7,3,1)$ 一循环差集正好是一个例子. 把这种差集的关联表镶嵌上一道全是黑色格子的曲尺边，作为第一行和第一列（见图10），得到的阵列有个好性质，就是任何两行（或两列）都有恰好一半的位置同是白色或同是黑色的格子. 在1868年英国数学家西勒维斯特(J. J. SYLVESTER)提出这样的一个趣味数学问题，想不到过了25年后，法国数学家阿达玛(J. HADA-

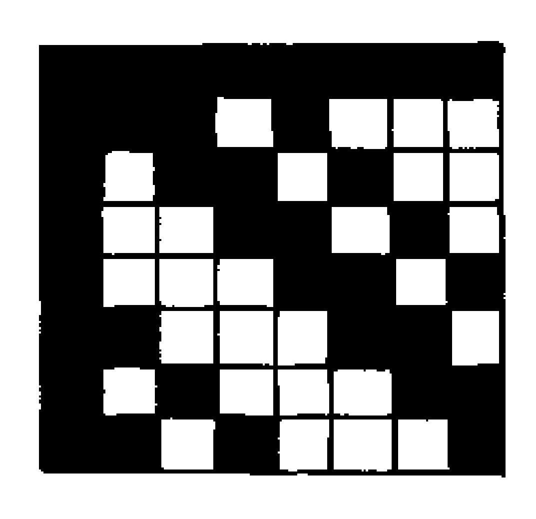


图10

MARD)研究行列式的极大值时竟又碰上它!把黑色格子和白色格子分别换作1和－1,得到的矩阵满足 $HH^T=H^TH=(4N)I$,这样的矩阵叫做阿达玛矩阵,阿达玛差集的名称便是这样产生的.

让我们又换一个角度看看范诺构形的关联表,这次把它看成是放置7个元在7个区组的方案,要求每个区组都有3个元,每一对元都在一个仅只一个区组内出现.更一般地,我们可以试寻找在 v 元集 S 内挑选某些 k 元子集(叫做区组)的方案,要求每个 t 元子集都恰好在 λ 个区组内出现.这样的一族 k 元子集 $\mathscr{D}$ 叫做一个 (v,k,λ)-t 设计.范诺构形的关联表提供了一个(7,3,1)-2设计.虽然 t 设计这个名字是到了1962年才因数学家晓治(D. R. HOGHES)的引进而流传,但这种组合数学对象却早在30年代已受到注意,主要原因是它在统计学上的试验设计非常有用.2设计也叫做平衡不完全区组设计(BALANCED INCOMPLETE BLOCKK DESIGN),简称为 BIBD,是英国统计学家叶斯(F. YATES)在1936年提出来研究的.当 BIBD 的参数 v 和 b 相同,它叫做 SBIBD,头一个字母表示对称(SYMMETRIC).$\lambda=1$的 SBIBD,即是$(k-1)$阶射影平面.$\lambda=1$的 BIBD,也叫做斯坦纳系(STEINER SYSTEM),因19世纪瑞士数学家斯坦纳(J. STEINER)的研究工作而得名.但其实最先提出这种问题的是一位英国牧师柯克曼(T. J. KIRKMAN):"一位女教师每天带领15名女学生去散步,她要求学生们排成三人一行,又要求任何两名学生在一周七天内恰好有一天排在同一行,它应该怎样安排呢?"有关各种区组设计的研究和构作,至今犹蓬勃不已,除了由于它在试验设计上的应用外,还因为它跟编码理论(CODING THEORY)和散在单群(SPORADIC GROUP)理论有密切关系.

5. 两两正交拉丁方完全组

看过第2节和第4节的叙述，读者大概明白了数学家并非为了请客吃饭才研究射影平面吧！在这一节我再介绍一种组合数学对象，并且通过它把10阶射影平面存在问题化成另一个形式. 无独有偶，这种数学对象又是与数学游戏有关.（也许这篇文章可以取题为“戏无益乎？”！）瑞士数学家欧拉（L. EULER）在1779年发表了一篇构作幻方（MAGIC SQUARE）的文章，引进了今天我们叫做拉丁方的阵列. 一个 N 阶拉丁方（LATIN SQUARE OF ORDER N）是个 N 行 N 列的矩阵，里面的元选自 N 个不同的符号（为方便叙述不妨写作0、1、2、…、$N-1$），条件就是在每一行和每一列全部 N 个符号都要出现. 例如 $\begin{bmatrix} 0 & 2 & 1 \\ 2 & 1 & 0 \\ 1 & 0 & 2 \end{bmatrix}$ 是个三阶拉丁方，但 $\begin{bmatrix} 0 & 2 & 1 \\ 2 & 1 & 0 \\ 0 & 2 & 2 \end{bmatrix}$ 却不是. 设 A 和 B 是两个 N 阶拉丁方，考虑它们在相应位置的元构成的 N^2 对有序偶，如果两两不同，我们便说 A 和 B 是正交的拉丁方. 例如 $\begin{bmatrix} 0 & 2 & 1 \\ 2 & 1 & 0 \\ 1 & 0 & 2 \end{bmatrix}$ 和 $\begin{bmatrix} 1 & 2 & 0 \\ 0 & 1 & 2 \\ 2 & 0 & 1 \end{bmatrix}$ 是正交的拉丁方，但 $\begin{bmatrix} 0 & 2 & 1 \\ 2 & 1 & 0 \\ 1 & 0 & 2 \end{bmatrix}$ 和 $\begin{bmatrix} 1 & 2 & 0 \\ 2 & 0 & 1 \\ 0 & 1 & 2 \end{bmatrix}$ 却不是，因为第一行第一列和第二行第三列的有序偶都是（0，1）. 欧拉在他的文章里指出不存在一对正交的6阶拉丁方，但他用游戏口吻说：“有6个军团，从每个军团选6名不同军

阶的军官. 怎样把这36名军官排成6行6列,要求每一行和每一列都有6名不同军阶且隶属不同军团的代表?”接着他还说:“我毫不迟疑下这样的结论,不存在一对正交的6阶拉丁方,而且这个结论还能推广至10阶、14阶、……的情况,即当阶是二乘某个奇数的情况.”欧拉可没有证明他的断言,后人管这个断言作欧拉猜想. 1900年塔利兄弟(G. TARRY, H. TARRY)穷举全部6阶拉丁方验算了猜想在6阶情况果然成立. 到了20年代,由于拉丁方在试验设计上的应用引起数学家的注意,欧拉猜想也就给提到议事日程来. 美国数学家麦尼殊(H. F. MACNEISH)在1922年甚至提出一个更强的猜想:设 $N=p_1^{r_1}\cdots p_m^{r_m}(N\geqslant 2)$ 是 N 的质因子分解式,则顶多只能找到 t 个两两正交的 N 阶拉丁方,t 是 $p_1^{r_1}-1$、…、$p_m^{r_m}-1$当中最小的数. 不难证明当 N 是质数幂时(即 $m=1$),这猜想是对的,因为一般而言,顶多只有 $N-1$个两两正交的 N 阶拉丁方,读者有兴趣试证明吗?后来数学家知道真的可以找到这样 t 个拉丁方,关键在于 N 是质数幂的情况,逐个 $p_i^{r_i}$ 的情况解决了,便可以合成 t 个两两正交的 N 阶拉丁方,详情不赘. 以“事后诸葛亮”的眼光看,质数幂的情况不难明白,但最先看到这种关系的洞察力,可叫人佩服,这份功劳归于原籍印度的美国数学家玻色(R. C. BOSE),他在1938年运用抽象代数中有限域的知识解答了这个问题.

定理4 若 N 是个质数幂,则有 $N-1$个两两正交的 N 阶拉丁方.

N 是质数幂,便有 N 元域 $F=\{a_0=0, a_1, \cdots, a_{N-1}\}$. 置 $a_ka_i+a_j$ 作第 k 个 $N\times N$ 矩阵中第 i 行和第 j 列的元. 直接验算可知每个矩阵是个拉丁方,且两两正交,故定理4得证.

在1958年,美国数学家派克(E. T. PARKER)找到至少四个两两正交的21阶拉丁方,推翻了麦尼殊猜想(按照该猜想顶多只

有两个这样的拉丁方)，玻色和他的学生西里克汉特(S. S. SHRIKHANDE)循着这个方向穷追猛打，数月后找到一对正交的22阶拉丁方，推翻了欧拉猜想. 同时，派克也找到一对正交的10阶拉丁方，然后他们三位数学家联手夹攻，终于在翌年证明了一条叫人极感诧异的定理：除 $N=2$和6以外，必有一对正交的 N 阶拉丁方. 这个发现竟上了当时(1959年4月24日)《纽约时报》的头条新闻!

但是，一组个数最多的两两正交拉丁方，至今仍是悬而未决的问题，特别地，如果有 $N-1$个两两正交的 N 阶拉丁方，我们把它叫做一个完全组，定理4是说当 N 是质数幂时，存在一个两两正交 N 阶拉丁方完全组. 玻色在同一篇文章里证明了另一条有趣的定理.

定理5 设 $N\geqslant 3$，存在一个两两正交 N 阶拉丁方完全组的充要条件是存在一个 N 阶射影平面.

虽然我不在这里证明这条定理，让我以一个实例来印证，好使读者看到它的内涵. 取一个两两正交3阶拉丁方完全组，由

$\begin{bmatrix}0&1&2\\1&2&0\\2&0&1\end{bmatrix}$和$\begin{bmatrix}0&1&2\\2&0&1\\1&2&0\end{bmatrix}$组成. 把相应位置的元构成有序偶写在该位置标号的右边，由此得到9点，如图11所示. 把这些点分成四组“平行线”，办法如下：选第一个位是0的点构成第一条线，第一个位是1的点构成第二条线，第一个位是2的点构成第三条线，这三条线是第一组；类似地，按照第二个位分别是0、1、2又取三条线，是第二组；按照第三个位分别是0、1、2又取三条线，是第三

A	0	0	0	0
B	0	1	1	1
C	0	2	2	2
D	1	0	1	2
E	1	1	2	0
F	1	2	0	1
G	2	0	2	1
H	2	1	0	2
I	2	2	1	0

图11

组；按照第四个位分别是0、1、2又取三条线，是第四组(见图12).现在，再添加四个“理想点”α、β、γ、δ，于是共有13个点.在第一组的每条线多添 α、在第二组的每条线多添 β、在第三组的每条线多添 γ、在第四组的每条线多添 δ，连同由 α、β、γ、δ 组成的线共有13条线.这13个点和13条线构成一个三阶射影平面，反过来，如果有一三阶射影平面，适当地赋予座标后，可以把上述步骤倒转过来构作一个两两正交三阶拉丁方完全组.

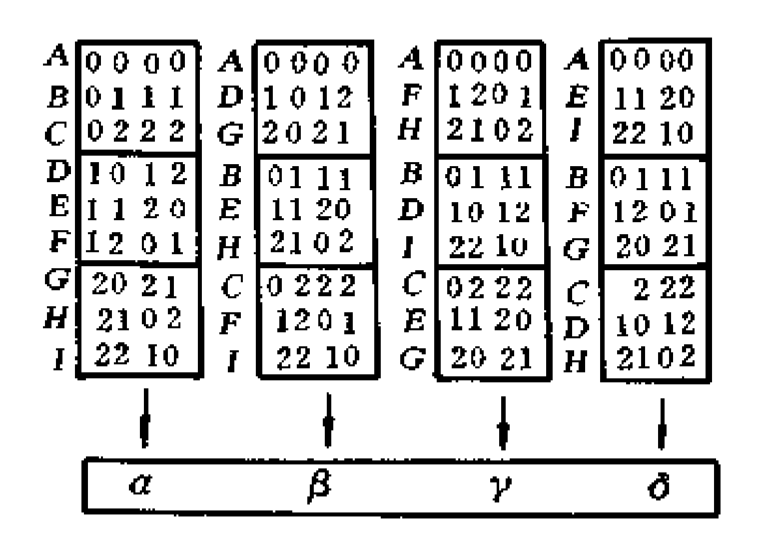


图12

从定理5可知10阶射影平面存在问题化为：有没有9个两两正交的10阶拉丁方？在60年代派克曾经构作了一个10阶拉丁方，估计有一百万个10阶拉丁方跟它正交，但可惜在这众多拉丁方当中竟找不着一对互相正交的！到目前为止，我们还不知道有没有三个两两正交的10阶拉丁方.

6. 不存在10阶射影平面：电脑证明

阅读了林永康教授惠寄来的多篇文章后，我看到他和他的

小组的研究历程，让我在这一节作个很简略的介绍. 有兴趣知道详情的读者可以参阅下面两篇文章：

C. W. H. LAM, *LITHIEL*, *S. SWIERCZ*, *THE NON—EXISTENCE OF FINITE PROJECTIVE PLANES OF ORDER* 10, PREPRINT, 1989(将于 Canad. J. Math 发表).

C. W. H. LAM, *THE END OF A FINITE PROJECTIVE PLANE OF ORDER* 10, PREPRINT, 1989(将于 Amer Math Monthly 发表)

要明白他们的工作，先要知道什么是一个码(CODE). 码是通讯科学上为了防范讯道受干扰引致的传输错误的设计，如果仅为了看明白这一节，可以把一个码看成是二元域上 n 维空间里的一个 k 维子空间，正确的术语是线性(n,k)码〔LINEAR(n,k)CODE〕. 它的向量叫做码字，码字里1的个数叫做该码字的重量(WEIGHT). 一个码的检错和纠错能力，视乎码字的最小重量，所以一个码的码字重量分布是很重要的研究目标，让我们以 W_k 表示重量是 k 的码字的个数.

如果存在一个10阶射影平面，它的关联矩阵的行可以看成是111个在二元域上的111维空间里的向量，它们生成的子空间是个码，记作 C. 在1990年阿斯莫斯(E. F. ASSMUS, JR.)和马森(H. F. MATTSON, JR.)提出研究这个码以求了解10阶射影平面，他们还证明了只用计算 w_{12}、w_{15}、w_{16}便能完全确定 C 的码字重量分布. 在1973年，麦威廉士(F. J. MACWILLIAMS)、史隆尼(N. J. A. SLOANE)和汤普森(J. G. THOMPSON)三人合力证明了 $w_{15}=0$. 过了10年后，林永康和他的小组证明了 $w_{12}=0$. 早在1974年卡特(J. L. CARTER)在他的博士论文里已经做了大部分关于 w_{16}的计算，经汤普森的怂恿，林永康等乘胜追击，在1986年完成剩下的计算，证明了 $w_{16}=0$. 于是 C 的码字重量

分布完全知道了，特别地，$w_{19}=24675$，换句话说，如果存在一个10阶射影平面，由它生成的码应该有24675个码字的重量是19．倒过来考虑，设10阶射影平面里的19点构成一个重量是19的码字，数学家知道这些点和某些线的相交构形有某种性质，于是一个方法是试图从这些“起点构形”出发，把它延伸为一个10阶射影平面的关联矩阵，成功的话便找到一个10阶射影平面，穷举全部“起点构形”后也延伸不成功的话，便证明了不存在10阶射影平面了．

林永康等计算了共有66个“起点构形”要考虑，其中凭推理知道21个是不能延伸的，另外的45个却只好借助电脑作验算了．当中有8个涉及的计算量很大，使用他们的大学里的电脑设备的话，估计要用上几十年至一百年！幸好在这个时候，他们得到位于美国普林斯顿的国防分析研究所（INSTITUTE OF DEFENSE ANALYSIS）的协助，允许他们利用那里的CRAY—IA型超级电脑在工余时间进行验算．从1986年秋季开始计算，直至1988年11月中，经过2000多小时的计算时间，答案终于出来了：不存在10阶射影平面．宣称这个重要发现时，林永康这样说：“由于使用了电脑验算，我们不应把这个结果视作在传统意义下的“证明”，它只是一个实验结果，也就不能避免产生实验错误的可能．话虽如此说，以下我们要举出理由说明存在仍然未给发现的10阶射影平面的可能性是极低的．”这些理由分为两方面，其一是电脑程序的处理，其二是硬件设备的检错．在程序方面，他们使用不同的程序去计算以资比较，有时甚至用手算来验证，同时又在程序中加了核算的步骤作保险．在硬件设备方面，超级电脑平均每1000小时计算时间会出错一次的，他们也的确曾经发现过这种错误，后来补算了．或者可以这样说，既然如果10阶射影平面存在的话，它可以从那么多码字延伸而

来（共有24675个重量是19的码字），但至今仍然没有一个10阶射影平面给发现，这便是一个有力的证据，显示它并不存在了.下一个待决定的情况是12阶射影平面存在与否，但据林永康说，沿用同样的手法使用目前的超级电脑去验算，恐怕以人有生之年也办不到了！

7. 后　　记

自从哈肯（W. HAKEN）和阿佩尔（K. APPEL）在1976年宣称他们借助电脑证明了四色问题（FOUR—COLOOR PROBLEM）后，电脑证明进入了数学讨论，并且引起争议. 反对的一方认为这不能算是数学证明，因为很难保证电脑不出错，而且更难确定出错的是电脑操作的毛病还是人为的纰漏；支持的一方则认为人手计算不见得没有机会出错，有些证明的繁复程度不遑多论，说不定电脑较人更小心呢. 反对的一方也认为数千年来数学证明都毋需借助电脑，将来亦无此需要；支持的一方却认为有些命题的证明可能除了验算全部情况外别无他法，以前它们不出现只因为以前没有电脑时人的计算能力未臻这个高度吧.

其实，如果我们不把证明的功能限于核实而更重视证明在说明阐释方面的作用的话，电脑证明叫人最不惬意者倒不是上面提及的几点，而是它顶多令人相信该命题成立，却没有令人明白为何该命题成立. 对于一个深信数学研究的主要目标乃追求理解的人来说，电脑证明只能起辅助作用，却不能带来犹如当年古希腊数学家阿基米德高喊 EUREKA 时的那份喜悦！

〔最近林永康就这点写了一篇文章，读者可以参阅，听听证

明者本人的意见：

C. W. H. LAM, *HOW RELIABLE IS A COMPUTER — BASED PROOF*? THE MATHEMATICAL INTELLIGENCER, VOL 12 (1990), 8—12.]